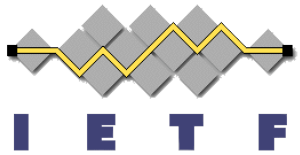
KARP WG

KARP Threats & Requirements
draft-ietf-karp-threats-reqs-01



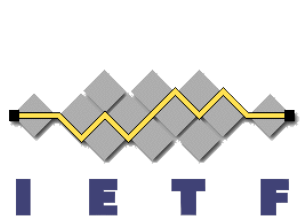
Gregory Lebovitz, Juniper
Manav Bhatia, Alcatel-Lucent
Russ White, Cisco

IETF 79, Beijing

What's changed?

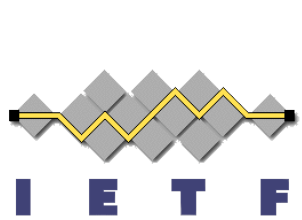
- Russ White, Cisco, joined author team.
- Abstract thinned, less redundant to design-guide and –framework
- 1.1 Terminology:
  - Updated PRF, KDF based on list feedback
  - Edited “Identity Proof”, “KMP” and “Traffic Key” based on re-reading

1.4 Incremental Approach



- Moved this text out of its various locations in “Goals” section, and into it’s own section.

3. Requirements for Phase 1



- Inter-connection replay protection – beefed up the definition
- Added:
  - 19 - Reveal as little info on wire as possible to avoid giving undo hints to a passive attacker
  - 20 – when using a group key, address issue of masquerading as a different peer.
  - 21 – if use IP addr as ID assertion, must protect IP in header

What else?

- Fixed many nits. Still a few comments on list left to address.
- Check for your comments? Send mail on list, but do so quickly, because…
- Design teams are starting to form and get to work