Keying and Authentication for Routing Protocols (karp)

IETF 86

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

Administrivia (5 minutes)

- Scribes (Meeting Minutes & Jabber)
    - We still need a Scribe
    - We still need a Jabber Scribe
- Blue Sheets

Welcome & Document Status - Chairs (10 minutes)

Core Document

- Database of Long-Lived Symmetric Cryptographic Keys – Dacheng Zhang (10 minutes)
- *Operations Model for Router Keying* – Sam Hartman (10 minutes)

Routing Protocol Analyses

- *OSPF WG Security Gap Analysis and Response* – Acee Lindem (10 minutes)

Key Management

- *Negotiation for Keying Pairwise Routing Protocols in IKEv2* – Dacheng Zhang (20 minutes)
- Automatic Key and Adjacency Management for Routing Protocols – Bill Atwood (10 minutes)

New RFCs

- RFC 6862
  - Keying and Authentication for Routing Protocols (KARP) Overview, Threats, and Requirements

- RFC 6863
  - Analysis of OSPF Security According to the Keying and Authentication for Routing Protocols (KARP) Design Guide

Current WG Drafts

draft-ietf-karp-routing-tcp-analysis-06

  Status: IESG Evaluation::Revised ID Needed. Authors hope to wrap up open issues in conversations this week.

draft-ietf-karp-crypto-key-table-06

  Status: Waiting for WG Chair Go-Ahead. Chair is giving WG a few days to review before forwarding to the AD.

draft-ietf-karp-ops-model-05

  Status: I-D Exists. Authors believe the I-D is ready for WGLC.

draft-ietf-karp-isis-analysis-00

  Status: I-D Exists. Recently accepted as WG I-D

draft-ietf-karp-bfd-analysis-00

  Status: I-D Exists. Recently accepted as WG I-D

Related Drafts

draft-mahesh-karp-rsvp-te-analysis-00

Status: Discussion on mailing list

draft-bhatia-karp-pim-gap-analysis-00

Status: Expired. Manav started this, and Toerless Eckert agreed to co-author but no further version has been published

draft-mahesh-karp-rkmp-04

Status: Requesting WG adoption

draft-chunduri-karp-kmp-router-fingerprints-03

Status: Requesting WG adoption

draft-tran-karp-mrmp-02

Status: Waiting on group key management strategy

draft-atwood-karp-akam-rp-03

Status: Asking for reviews from the WG

Charter Goals Review

- We've made good progress on the goals (albeit not in the expected timeframe).

  – Protocol analyses for all RPs are covered except for LMP. (Any volunteers?)

  – Ops Model I-D is moving along to provide operator advice

  – Automated key management work is being proposed, multiple individual efforts in progress.

- Let's get to work ….