Keying and Authentication for Routing Protocols (karp)

IETF 84

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

- *Operations Model for Router Keying* – Dacheng Zhang (10 minutes)

Key Management

- *Database of Long-Lived Symmetric Cryptographic Keys* – Dacheng Zhang (20 minutes)
- *Using IKEv2 with TCP-AO* - Uma Chundauri (15 minutes)
- *Simplified Authentication Method for KARP KMP* - Uma Chundauri (15 minutes)
- *Automatic Key and Adjacency Management for Routing Protocols* – Bill Atwood (15 minutes)

Current WG Drafts

draft-ietf-draft-ietf-karp-threats-reqs-05

   Status: IESG Evaluation::Revised ID Needed

draft-ietf-karp-ospf-analysis-02

   Status: Submitted to IESG for Publication. Doc Shepherd Follow-up Underway

draft-ietf-karp-routing-tcp-analysis-00

   Status: WG Consensus: Waiting for Write-Up. Doc Shepherd Follow-up Underway

draft-ietf-karp-ops-model-03

   Status: I-D Exists.

draft-ietf-karp-crypto-key-table-03

   Status: I-D Exists.

Milestone Discussion

- We are behind in our milestones, but more importantly we do not have WG drafts these protocols:
  - RSVP-TE
  - ISIS
  - BFD
  - LMP

Next Steps

- For the analysed protocols, we need to take the next stop in analysis

  – Some protocol I-Ds and RFCs published to address the gaps in the analyses, but do they close all of the gaps?

  – Key management analysis is on-going as part of the key management solution work

Key Management

- The majority of our time today will be spent on key management
  - It will be important to gain consensus soon on directions for key tables, protocol flows, and high level frameworks