Keying and Authentication for Routing Protocols (karp)

IETF 85

Fishing Atlanta-area Carp Flats

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* – Sam Hartman (15 minutes)

Routing Protocol Analyses

- *KARP IS-IS security gap analysis* – Uma Chunduri (15 minutes)
- *Analysis of Bidirectional Forwarding Detection (BFD) Security According to KARP Design Guide* – Mahesh Jethanandani (15 minutes)

Key Management

- *TCP Authentication Option Master Key Tuple negotiation in IKEv2* – Dacheng Zhang (20 minutes)
- *KARP KMP: Simplified Peer Authentication* – Uma Chundauri (20 minutes)

Current WG Drafts (1of 2)

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

Status: IESG Evaluation::AD Followup (Sean Turner to evaluate whether -06 adequately addresses his DISCUSS)

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

Status: In Last Call (ends 2012-11-19)

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

Status: I-D Exists. In WG Last Call (ends 2012-11-12) Please add statements of support and/or post comments to the WG list.

draft-ietf-karp-ops-model-03

Status: I-D Exists. Authors believe the I-D will be ready for WGLC before IETF 86.

Current WG Drafts (2 of 2)

draft-ietf-karp-ospf-analysis-02

Status: Waiting for AD Go-Ahead. IETF LC complete, Stewart Bryant waiting for authors to confirm the intent of wording clarifying one sentence.

Original text: "*The OSPFv2 replay mechanism does not handle packet priorities as described. If packets are processed out-of-order, then if the sequence number increases, packets processed later will be discarded.*"

Acee Lindem's explanation: "*The OSPFv2 replay mechanism does not handle prioritized transmission of OSPF Hello and Link State Acknowledgement packets as recommended in [RFC 4222]. When OSPF packets are transmitted with varied prioritization, they can arrive out-of-order resulting in packets with lower prioritization being discarded.*"

Other protocol analyses

- PIM: A draft I-D for PIM is being updated, but was not ready for this meeting.
    - – Manav Bhatia (current author)
    - – Toerless Eckert (collaborating)
- RSVP-TE & LMP: Still looking for authors
    - – Mahesh Jethanandani (volunteered)

Key Management

- The WG may be coming to consensus on an approach for TCP-AO automated key management (AKM)
  - Still some discussion on how AKM interacts with the *routing protocols* and *Crypto Key Tables*
- Several approaches still proposed for automated group key management