KARP Key Management

Charter Review

Key Management Charter Deliverables

- Define one or more frameworks describing the common elements for modern authentication in routing protocols
  - draft-ietf-karp-crypto-key-table-09
- Specify automated key management needs for routing protocols
  - No Automated Key Management (AKM) WG drafts have been accepted to date

Manual Keys vs. AKM

- At the outset, it was understood that operators distribute integrity keys manually, and this was not going to change in the short term
- It was also believed that manual keys were an operational burden, and did not provide the same quality of security as keys generated from AKM

AKM Drafts discussed

- IETF 79 (Beijing)
  - draft-hartman-mrkmp-00
  - draft-liang-karp-auto-sa-management-rp-00
- IETF 80 (Prague)
  - draft-hartman-mrkmp-01
  - draft-liang-karp-negotiation-kmp-00
- IETF 81 (Quebec City)
  - draft-mahesh-karp-kmprp-00
  - draft-zhang-karp-rkmp-00
- IETF 82 (Taipei)
  - draft-chunduri-karp-using-ikev2-with-tcp-ao-00
  - draft-mahesh-karp-rkmp-00
  - draft-tran-karp-mrmp-00

AKM Drafts discussed

- IETF 83 (Paris)
  - draft-mahesh-karp-rkmp-01
  - draft-hartman-karp-mrkmp-04
  - draft-tran-karp-mrmp-01
- IETF 84 (Vancouver)
  - draft-chunduri-karp-using-ikev2-with-tcp-ao-00
  - draft-chunduri-karp-kmp-router-fingerprints-00
  - draft-atwood-karp-akam-rp-00
- IETF 85 (Atlanta)
  - draft-mahesh-karp-rkmp-02
  - draft-chunduri-karp-kmp-router-fingerprints-01
- IETF 86 (Orlando)
  - draft-mahesh-karp-rkmp-04
  - draft-atwood-karp-akam-rp-00
- IETF 87 (Berlin)
  - draft-atwood-karp-aapm-rp-00

WG Calls for adoption

- draft-chunduri-karp-kmp-router-fingerprints-03
  - Call duration: July 15, 2013 – July 29, 2013
  - No comments on the list
- draft-mahesh-karp-rkmp-04
  - Call duration: July 29, 2013 – August 19, 2013
  - One neutral comment on the list, no support given
  - Call extended: August 19, 2013 – August 26, 2013
  - No comments on the list

Observations by Chairs/ADs

- Apparently there is no interest in the WG for actually taking on AKM for RPs other than the authors
- Speculations
  - Operators have solved the operational problems elsewhere
  - Operator still don’t trust AKM

WG Discussion

- Some useful things you could say
  - Whether you think the chairs are right or wrong, and why
  - If you're an operator, whether you think there's any value of specifying standards in this area at all
  - Most importantly, whether or not you support the WG moving forward specifying AKM for RPs