IPsec and IKE Document Roadmap

<draft-ietf-ipsecme-roadmap-00.txt>

Sheila Frankel, NIST

sheila.frankel@nist.gov

Suresh Krishnan, Ericsson

suresh.krishnan@ericsson.com

Goals

- Identify all IPsec/IKE-related RFCs and their inter-relationships
- Brief description of each RFC
- Descriptive doc vs. Prescriptive

Topic Headings

- IPsec/IKE Background Information
- IPsec Documents
- IKE Documents
- Cryptographic Algorithms and Suites
- IPsec/IKE for Multicast
- Outgrowths of IPsec/IKE
- Other Protocols that use IPsec/IKE

Status and Plans

- -00 Draft Published on 12/22/08
- Missing text
  - Introductions to several sections
  - Descriptions of RFCs in several sections
- -01 Draft planned before March IETF
  - Will include missing text
  - Incorporate comments from mailing list

Comments on -00 Draft

- IPsec SA vs. Child SA
- Add Requirements levels for other docs?
  - How detailed? RFC? Individual features?
- RFCs not widely adopted
  - IPsec config PIM (RFC3585)
  - IPsec SPD config MIB (RFC4807)
  - IPsec trans mode for Dynamic Rtg (RFC3884)
  - Others?

Comments on -00 Draft (cont'd)

- RFCs with few/no known implementations
  - KINK (RFCs 3129, 4430)
    - Included in racoon – others?
  - IPsec KEY (RFC4025)
  - DHCP Config of IPsec tunnel mode (RFC3456)
  - Others?
- Yaron: suggested text, additions and deletions

Comments on -00 Draft (cont'd)

- Missing RFCs
  - Multicast extensions to sec arch: RFC5374
  - HMAC-MD5: RFC22403
  - RoHC
    - RFC5225 - ESP profile for RoHCv1
    - RFC3095 – ESP profile for RoHCv2
    - 3 IPsec/IKE-related Drafts in IETF Last Call
    - RFC4995 – no mention of IPsec – omit
  - Other RFCs (besides PANA) that use prf+?

Input Requested

- Missing topics
- Missing RFCs
- Corrections
- Level of detail in RFC descriptions
- Requirements levels for crypto algorithms – please review and comment