IPsec and IKE Document Roadmap

<draft-ietf-ipsecme-roadmap-04.txt>

Sheila Frankel, NIST

Suresh Krishnan, Ericsson

Issue #1

- Combined algorithms for IKEv1 and IPsec-v2
  - AES-CCM, AES-GCM: IANA #’s in IPsec-v2 registry
  - Can IKEv1 negotiate combined algorithms for IPsec-v3 and generate the salt?
  - New requirement levels for AES-GMAC
    - IKEv1: N/A ➔ optional
    - IPsec-v2: undefined ➔ AH-v2 optional, ESP-v2 N/A
  - New requirement levels for AES-GCM
    - IKEv1: N/A ➔ optional

Issue #2

- Does IKEv2 truncate its ICV?
  - RFC 4306: “For integrity algorithms based on a keyed hash, the key size is always equal to the length of the output of the underlying hash function.”
    - No mention of truncation
  - IKEv2 uses the same algorithms for the IKE SA and the child SA
    - RFC 4307: only SHA RFC cited in HMAC-SHA-1-96
    - For IKEv2 states: “HMAC-SHA1 MUST be implemented”

Issue #3

- Use of AES-XCBC in IKE
  - RFC 4109: AES-XCBC, AES-XCBC-PRF: SHOULD for IKEv1
    - Problem: no IKEv1 IANA value
  - RFC 4307: AES-XCBC-PRF SHOULD+ for IKEv2, AES-XCBC optional (not mentioned)
  - Questions:
    - Can they be used in IKEv1?
    - If so, what does the proposal look like?

Issue #4

- Internet Drafts included in roadmap
  - IPsecME (7)
  - IPsec/IKE Benchmarking (2)
  - BTNS (1)
  - ECP for IKE (1)
  - MIP6 (1)
- Added ROHC for IPsec/IKE (3)
- Questions:
  - BEET?
  - Expired drafts?
    - Draft-dukes-ike-mode-cfg
    - Draft-beaulieu-ike-xauth

Issue #5

- Camellia for IKEv2: undefined (no RFC)
  - Question: Should we change any of these req levels to optional, based on other existing RFCs?
    - Camellia-CBC: generic CBC reqs in RFC4306
    - Camellia-CTR: extend new AES-CTR draft to cover other CTR algs
    - Camellia-CCM: RFC 5282 (Combined mode algs in IKEv2)