IKEv2bis
Some open issues

Paul Hoffman, VPN Consortium

IPsecME WG interim meeting, 2009-05-05

v.02

#9 Notification when creation of CHILD SA fails (1)

- General agreement that you don't nuke the IKE SA
- No consensus on whether or not the error message should be encrypted and/or MAC'd

#9 Notification when creation of CHILD SA fails (proposed text)

- Note that although the IKE_AUTH messages are encrypted and integrity protected, if the peer receiving this notification has not authenticated the other end yet (or if the peer fails to authenticate the other end for some reason), the information needs to be treated with caution. More precisely, (assuming that the MAC verifies correctly) the sender of the error indication is known to be the responder of the IKE_SA_INIT exchange, but the sender's identity cannot be assured.

#12 Traffic selectors when rekeying

- New text was proposed.
- It was pointed out that
  - The text has a new MUST
  - It assumes that the encryption algorithm and so on will be the same

#26: Missing treatment of error cases

- Should we extend section 2.21?
  - Errors happening before authentication
  - Errors in the IPsec SA creation on IKE_AUTH
  - Describe which errors are so fatal that they cause the whole IKE SA to destroyed
- Nothing on the list yet for these

#57: Clarify D-H transform (1)

- 3.3.2: there is no explanation here or elsewhere that the D-H transform for ESP and AH is used for PFS.
- Paul doesn’t think it belongs in 3.3.2, and also doesn't agree that the transform is “the D-H transform for ESP and AH is used for PFS”

#57: Clarify D-H transform (proposed text)

- Although ESP and AH do not directly include a Diffie-Hellman exchange, a D-H group MAY be negotiated for the Child SA. This allows the peers to employ D-H in the CREATE_CHILD_SA exchange, providing Perfect Forward Secrecy for the generated Child SA keys.

#58: Access control: add ref to IPsec architecture

- Section 3.5 is extremely liberal on what access control policies people can implement, but that's too late to change now. However, we CAN at least add a reference to RFC 4301, Sec. 4.4.3.1 (as was done in RFC 4945, pki4ipsec).

#58: Access control: add ref to IPsec architecture (proposed text)

- The Peer Authorization Database (PAD) as described in RFC 4301 describes the use of the ID payload in IKEv2 and provides a formal model for the binding of identity to policy in addition to providing services that deal more specifically with the details of policy enforcement. The PAD is intended to provide a link between the SPD and the IKE security association management. See RFC 4301, Section 4.4.3 for more details.