IKEv2bis Status

IPSECME WG, IETF 72, Dublin

Paul Hoffman, VPN Consortium

Overview

- Where we are
- Where we want to be
- How to tell when we got there
- Getting there more efficiently

Current status of the draft

- Current is draft-hoffman-ikev2bis-03
  - Obsoletes IKEv2 (RFC 4306) and the IKEv2 clarifications (RFC 4718)
- Have already started draft-ietf-ipsecme-ikev2bis-00
- We think it is in good shape, but it is not complete

Some open issues, in no particular order

- The specification does not say which messages can contain N(SET_WINDOW_SIZE)
- Do we want an appendix that is all the changes from 4306? Who will decide which are important enough to list?
- Want to include material from Jari Arkko's "Effects of ICMPv6 on IKE and IPsec Policies"
- Section 2.6.1: Clarify the "MUST NOT fail"
- Section 3.3.6, second paragraph, hard to pick a proposal with a DH you don't like

How do we get more input?

- Not many reports coming out of either formal or in-lab interop testing
- What's the state of IPv6 in IKEv2?
- What about EAP methods?
- What do we hear from customers using IKEv2?

What is the end state?

- How do we tell when it is complete?
  - This is a hard question, given the lack of deployed implementations other than OEMs
  - Suggestions to the chairs are welcome
- What do we expect to happen in WG last call?
- Who else should we call in?

We could use another author

- Pasi is busy, and that is a good thing
- He will still review draft diffs, but cannot lead the effort like he has done in the past
- We could use another author
- Strong preference is an implementer who has done IKEv2 and is still doing IKEv2

Obligatory last slide

- Questions: now or online
- Offers to be co-author: offline during this week or in email to Yaron and I