Handing Over Child SAs Following Re-Authentication in IKEv2

Yoav Nir

Why?

- IKE implementations are required to periodically re-authenticate
  - Risk mitigation from stolen machines or revoked certificates
  - Holdover from IKEv1 where this was tied into re-keying.
- IKEv2 does not have a way to repeat authentication
  - It's just the initial exchange again + deleting the old.

Why?

- Child SAs are tied to a parent IKE SA
  - When it's deleted, they're gone.
- Following re-authentication, there's a need to re-create multiple child SAs.
- IKE SAs can have thousands of child SAs.
  - Mostly a lab scenario, but with multiple parallel SAs as allowed by RFC 5996 and prescribed by RFC 6311, there can legitimately be many.
- Down time

Why?

- For IKE SA Rekeying child SAs are transferred to the new SA.
- No such transfer exists for re-authentication
- This draft aims to fill this gap.

How?

- New notification - HAND_OVER_CHILD_SAS
  - Sent after renegotiation, within the **old** IKE SA.
  - Identifies the **new** IKE SA.
  - Sent along with the DELETE for the old IKE SA.
  - Tells peer to move old child SAs relating to this old IKE SA to the new IKE SA.
  - Both peers must agree for the move to happen.

Security Considerations

- Neither side should initiate or agree to the transfer unless the authenticated identities in the old and new IKE SAs match
- Otherwise logging and authorizations could be based on wrong identity
- How identities are matched is a local matter, and not specified in the document.