IKEv2 Support for Child SA PFS Policy Information

draft-pwouters-ipsecme-child-pfs-info-02

Paul Wouters (paul.wouters@aiven.io)
Valery Smyslov (svan@elvis.ru)

IETF 124

Problem Description

- When IKE SA is initially created, an initial Child SA is created as well
- For initial Child SA no separate Key Exchange (KE) is performed, thus the KE method is not negotiated at that time
- When the initial Child SA is later re-keyed (or a new Child SA is created), peers have to negotiate a KE method for Child SA for the first time since the IKE SA was created
- If peers have mismatched policy for Child SA KE methods, the negotiation will fail
- This can happen long after the initial SA is created, making it difficult to diagnose and fix the problem

Proposed Solution

- RFC 7296 prohibits the presence of KE method transforms (other than NONE) in SA payload in IKE_AUTH:

> Note that IKE_AUTH messages do not contain KEi/KEr or Ni/Nr payloads. Thus, the SA payloads in the IKE_AUTH exchange cannot contain Transform Type 4 (Diffie-Hellman group) with any value other than NONE. Implementations SHOULD omit the whole transform substructure instead of sending value NONE.

- We propose to lift this prohibition so that the full set of Child SA transforms is negotiated in IKE_AUTH, as in CREATE_CHILD_SA

More about Proposed Solution

- The processing of KE method transforms is the same as for other Child SA transforms
  - if Child SA policies are incompatible (including KE methods), the Child SA is not created with `NO_PROPOSAL_CHOSEN` returned, as per RFC 7296
    - the problem get known **immediately** (at the time initial Child SA is being created)
  - if initial Child SA is successfully created then peers can be sure that they have compatible Child SA policies for future Child SA rekeys

Proposed Solution Details

- The KE method negotiated this way is not used at all in the protocol, peers can immediately throw it away; the only thing that matters is whether the negotiation succeeded or not
  - peers can use it in other IKE extensions, like draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt
- If Child SA policy on any peer is later changed, then peers generally can no longer be sure that their policies are compatible
  - this is not specifically related to KE methods
  - in some cases (when new policy is a superset of an old one) this is not a problem
  - peers generally should re-establish SAs when policy changes

More Proposed Solution Details

- Peers have to negotiate this extension in IKE_SA_INIT via new notification `CHILD_SA_PFS_INFO_SUPPORTED`
  - no need to update RFC 7296
- If a peer is not going to re-key initial Child SA or create additional SAs (e.g., the SA is short-lived), it should not negotiate this extension
  - as it increases risk that initial Child SA would fail if Child SA policies disagree only on KE methods
- When RFC 9370 is supported by the peers, then “negotiation of KE method” means “negotiation of KE and AKE[1..7] methods”

Adoption?

- The WG decision was that draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt "Optimized Rekeys in the Internet Key Exchange Protocol Version 2 (IKEv2)" should rely on this mechanism
  - draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt normatively references this draft
  - It was expected that this draft would be adopted as WG document to make progress with draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt
- We believe the draft is ready for adoption call

Thanks!

Comments?

Questions?