IKEv2 Fragmentation

draft-ietf-ipsecme-ikev2-fragmentation-00

Valery Smyslov
svan@elvis.ru

IETF 87

Overview

- Problem: there are network environments that drop IP fragments. As some IKE messages often get fragmented due to their size, this doesn't allow IKE to succeed.
- Solution: avoid IP fragmentation by pre-fragmenting messages on IKE level.
  - DoS attack mitigation: protect each fragment with ICV. To do this SKEYSEED must already be computed.
    - only messages containing SK Payload can be fragmented

Protocol outline

- Unencrypted content of SK Payload is split into chunks, each chunk becomes the content of the newly introduced SKF Payload and gets the same protection as in SK Payload.
- Each SKF Payload is prepended with IKE Header, making IKE Fragment Message. All IKE Fragment Messages are sent at once to the peer.
  - All Fragment Messages bear the same Message ID
- Peer receives all IKE Fragment Messages, verifies them, decrypts content of each SKF Payload and then reassembles unencrypted content of the original SK Payload.

Limitations

- IKE Messages containing no SK Payload cannot be fragmented.
  - IKE_SA_INIT messages cannot be fragmented.
    - not a big deal as it is supposed to be small enough.
  - IKE_SESSION_RESUME messages cannot be fragmented.
    - use smaller ticket (e.g. by reference).
    - it is supposed that in case of IKE_SESSION_RESUME failure implementation will roll back to IKE_SA_INIT.
- If (fictional) IKE Message contains both unencrypted Payloads and SK Payload, only content of SK Payload get fragmented.
  - currently no IKE Exchange defines such Messages.

Open issues

- PMTU Discovery mechanism can be added to the protocol. Is it really needed?
  - IKE is not a bulk transfer protocol, thus size of its messages can be suboptimal
  - This option will add some (not much) complexity to the protocol and make it a bit less efficient
  - On the other hand, PMTU Discovery may allow IKE to operate in network environments with MTU less that 576 bytes.
    - Are there many of them?

Thanks

- Comments? Questions?
- Please review and send feedback to WG and author.