Re-direct Mechanism for IKEv2

IPSECME, IETF 74

Vijay Devarapalli (vijay@wichorus.com)
Kilian Weniger (kilian.weniger@googlemail.com)

Issues addressed Since the Last IETF

- Delete of SAs after REDIRECT
- REDIRECT_ACK payload
- The use of Redirect mechanism between IKEv2 peers
- DoS attacks using REDIRECT messages

Delete of SAs after REDIRECT

- Once the client receives the REDIRECT message from the gateway, it sends an acknowledgement to the gateway
- The client MUST delete the IKEv2 SA and the IPsec SAs (if any)
- If client does not, the gateway may delete the SAs
  - The gateway must allow sufficient time for the client to authenticate and establish security associations with the new gateway
- In both cases an explicit INFORMATIONAL message with DELETE payload is sent

REDIRECT_ACK payload

- □ An explicit REDIRECT_ACK is not required for gateway-initiated redirects
- □ An empty INFORMATIONAL message is used to acknowledge the REDIRECT from the gateway
- □ REDIRECT_ACK notification payload removed

Redirect between IKEv2 Peers

- There was a proposal to use the REDIRECT mechanism between any two IKEv2 peers
  - The document mainly focuses on client-gateway scenarios
- Consensus was to restrict this to the case where the original responder redirects the original initiator to another responder

DoS attacks using REDIRECT messages

- □ It is possible for an attacker to inject IKE_SA_INIT responses with REDIRECT payload and causes DoS attacks on the initiator
- □ Proposal is to have the responder echo the Nonce from the Ni payload in the REDIRECT payload
- □ The initiator matches the nonce in the REDIRECT payload with the nonce it sent in the Ni payload

Open Issue – Redirect and PAD entries

- When a gateway redirects the client to another gateway, is the new gateway subject to the same PAD entry or is a new PAD entry created for the new gateway?
  - Discussion on the mailing list supports the view that the new gateway is subject to the same PAD entry
- However, a scenario where GW1.example.com redirects the client to GW2.example.com needs to be supported for the REDIRECT message to be useful
  - Having all the gateways share the same FQDN is too limiting
  - One solution is to add all the gateways to the PAD entry on the mobile node
    - But this creates an issue when the service provider adds or removes gateways
- Proposed Solution:
  - Add text that says the original gateway and the new gateway are subject to the same PAD entry
  - To support the scenario above, have a a wild card that says *.example.com in the PAD entry on the client

Open Issue – Redirect during IKE_AUTH

- Redirect during IKE_AUTH exchange was added to the document
  - If re-direct is based on the user’s subscription profile or the client-indicated IDr, then the re-direct has to happen during the IKE_AUTH exchange
- REDIRECT payload is sent in the IKE_AUTH response
- If EAP or Multiple Authentications [RFC 4739] is used, the IKE_AUTH exchange is much more complicated
  - The gateway might decide to redirect based on the EAP authenticated ID, interaction with the AAA server or due to interaction with the external authentication server
  - Solution alternative 1
    - The gateway completes the IKE_AUTH exchange
    - An INFORMATIONAL message with the REDIRECT payload is then sent
  - Solution alternative 2
    - The gateway sends the REDIRECT payload in the IKE_AUTH response that also carries the EAP Success message

Open Issue – Redirect and the Security Associations

- If REDIRECT payload is sent during IKE_SA_INIT exchange, the IKEv2 SA is not created
- If the REDIRECT happens during the IKE_AUTH exchange, is the IKEv2 SA valid?
  - DH completed, but authentication has not happened yet
  - Assume IKEv2 SA is created and needs to be torn down?
  - IPsec SA is not created
- If EAP is used the REDIRECT goes along with EAP Success
  - Assume both IKEv2 SA and IPsec SAs are created?