A Childless Initiation of the IKE SA
draft-nir-ipsecme-childless-01

Yoav Nir
Hannes Tschofenig
Hui Deng
Raj Singh

November, 2009
What the Document Proposes

A simple extension to the initial IKE exchanges.

In IKE_SA_INIT, the responder signals support for this extension.

In IKE_AUTH initiator does not send payloads related to the Child SA:

- Security Association
- Traffic Selectors
- Various notifications
Regular IKE_AUTH

request    --> IDi, [CERT+],
[ N(INITIAL_CONTACT) ],
[ [N(HTTP_CERT_LOOKUP_SUPPORTED)], CERTREQ+ ],
[ IDr ],
AUTH,
[ CP(CFG_REQUEST) ],
[ N(IPCOMP_SUPPORTED)+ ],
[ N(USE_TRANSPORT_MODE) ],
[ N(ESP_TFC_PADDING_NOT_SUPPORTED) ],
[ N(NON_FIRST_FRAGMENTS_ALSO) ],
SA, TSi, TSr,
[ V+ ]

response    <-- IDr, [CERT+],
AUTH,
[ CP(CFG_REPLY) ],
[ N(IPCOMP_SUPPORTED) ],
[ N(USE_TRANSPORT_MODE) ],
[ N(ESP_TFC_PADDING_NOT_SUPPORTED) ],
[ N(NON_FIRST_FRAGMENTS_ALSO) ],
SA, TSi, TSr,
[ N(ADDITIONAL_TS_POSSIBLE) ],
[ V+ ]
Modified IKE_AUTH

request \(--\>\) IDi, [CERT+],
  [N(INITIAL_CONTACT)],
  [[N(HTTP_CERT_LOOKUP_SUPPORTED)], CERTREQ+],
  [IDr],
  AUTH,
  [CP(CFG_REQUEST)],
  [N(IPCOMP_SUPPORTED)+],
  [N(USE_TRANSPORT_MODE)],
  [N(ESP_TFC_PADDING_NOT_SUPPORTED)],
  [N(NON_FIRST_FRAGMENTS_ALSO)],
  SA, TSi, TSr,
  [V+]

response \(<--\) IDr, [CERT+],
  AUTH,
  [CP(CFG_REPLY)],
  [N(IPCOMP_SUPPORTED)],
  [N(USE_TRANSPORT_MODE)],
  [N(ESP_TFC_PADDING_NOT_SUPPORTED)],
  [N(NON_FIRST_FRAGMENTS_ALSO)],
  SA, TSi, TSr,
  [N(ADDITIONAL_TS_POSSIBLE)],
  [V+]
What the Document Proposes

- The result is an authenticated IKE SA.
- There is no Child SA.
- Depending on the use case, the IKE SA may later be used to create Child SAs, or not.
  - Signal this with a notification?
Why? - Remote Access

The usual IPsec way is to create IKE and Child SAs as needed. This is fine for gateways, but is inconvenient for human users.

You don't want the remote access client demanding your credentials just because the mail client is trying to reach the IMAP server.

When it's convenient for the user, she enters her credentials, and creates a stand-by IKE SA.

When IPsec needs an SA, only a non-intrusive CREATE_CHILD_SA exchange is done.
Sometimes we have a physically secure network, where we don't worry about eavesdroppers or packet injectors.

We do, however, want to identify who is on the other side of the line.

An IKE_AUTH exchange can authenticate the peer, but we really don't need a Child SA.
Why? - Location Awareness

Sometimes we want a remote access client to not encrypt when it is in a secure network (say, in the office)

We still want authentication, to run a location detection protocol

See the Secure Beacon draft
Why? - More Reasons

- Monitoring the peer's liveness using liveness check (without IPsec traffic)
- Detecting the presence of a NAT box between two IP hosts.
- EAP-IKEv2
- A future extension of “IKE Extractors”?  
  - Like TLS extractors...
Why this should be a WG draft

Different usage scenarios:

- Remote Access
- Regular VPN
- Private networks

Different industries

- Network Security
- Telephony

Potentially conflicting requirements

Some open questions