IKEv2 Session Resumption

http://www.ietf.org/internet-drafts/draft-ietf-ipsecme-ikev2-resumption-01.txt

For the IPSECME Virtual Interim Meeting

Note: This slide set uses the Yanone Kaffeesatz Thin font (see http://www.yanone.de/typedesign/kaffeesatz/) that can be downloaded from http://www.yanone.de/cgi-bin/download.pl?file=kaffeesatzfont

Issue#75: Make "by reference" a first class citizen

- All the text you captured assumed the ticket contain a value NOT a reference. Basically in order to be clear enough and reduce a lot of exchange, the draft is written with one type of ticket is in mind, "TICKET with VALUE".
- I suggest that the draft be rewritten with both types of tickets in mind as the draft itself allows.
- See http://www.ietf.org/mail-archive/web/ipsec/current/msg03369.html and related posts.

STATUS: Went through the document and made editorial changes.

Issue#74: Extend IKE_SA_INIT instead of new exchange type

- Use IKE_SA_INIT with a ticket payload, instead of defining a new exchange type.
- Main reasons: - Simpler implementation, adding a new exchange requires a lot of new code. - More efficient protocol of the responder *does not* implement this extension. - Similar to RFC 5077 (TLS stateless resumption).
- See http://www.ietf.org/mail-archive/web/ipsec/current/msg03356.html and follow ups.

STATUS: Discussions on the list and essentially two camps with different view

Issue#73: Ticket location: prefer server-side ticket

- The document should recommend "by reference", in preference to "by value" tickets; or make "by reference" a MUST, and "by value" a SHOULD/MAY. Mainly for the following two reasons:
- - Less bandwidth, by not sending the ticket. - IKEv2 messages, especially the first one, had better not be fragmented.
- See http://www.ietf.org/mail-archive/web/ipsec/current/msg03355.html and numerous follow-ups.

STATUS: Discussions on the list and rejected.

Issue#70: Ticket lifetime - explicit or not? (and ticket push from gateway)

- Current approach:
  - Gateway attaches a lifetime field to the ticket. Client knows the lifetime of the ticket.

- Alternative approach:
  - Lifetime local issue and when invalid ticket is presented then it is rejected.

STATUS: Open

When tickets expire how to obtain a new ticket?

- Option 1: Obtain ticket when new IKE SA is created only.
- Option 2: Client requests new tickets before they expire.
- Option 3: Gateway pushes tickets to the client before they expire.
- Option 4: Make it a policy decision and let the two parties choose what they want.

- The issue is a bit related to the question on how long the ticket lifetime would typically be.

STATUS: Open

Not-discussed items

- Issue#77: Identities in draft-ietf-ipsecme-ikev2-resumption
- Issue#76: IPsec child SAs during resumption
- Issue#69: Clarify behavior of SPI and sequence numbers