IKE Session Resumption

draft-ietf-ipsecme-ikev2-resumption

Yaron Sheffer,
Hannes Tschofenig

IPsecME Virtual Interim, Sep. 22, 2009

Two Recent Revisions

- -07 following AD review
- -08 following IETF LC, secdir and gen-art reviews

- Improved description of ticket by ref/value
- The gateway *always* supports IKE_SA_RESUME
- SPIs are unique, not necessarily random
- Vendor ID is resent on resumption
- Detecting resumption is out of scope, nevertheless added some security guidance
- Ticket reuse: mostly bad for privacy, so enforcement on gateway is only a SHOULD