draft-ietf-hip-base-01

Major changes since -00 and open issues

IETF 61, Washington DC

Petri Jokela
NomadicLab, Ericsson Research Finland
petri.jokela@ericsson.com

draft-ietf-hip-base-01.txt

- http://hip4inter.net -> Documentation -> roundup
  - Issue tracker (also for some other drafts)
  - Development versions of the draft

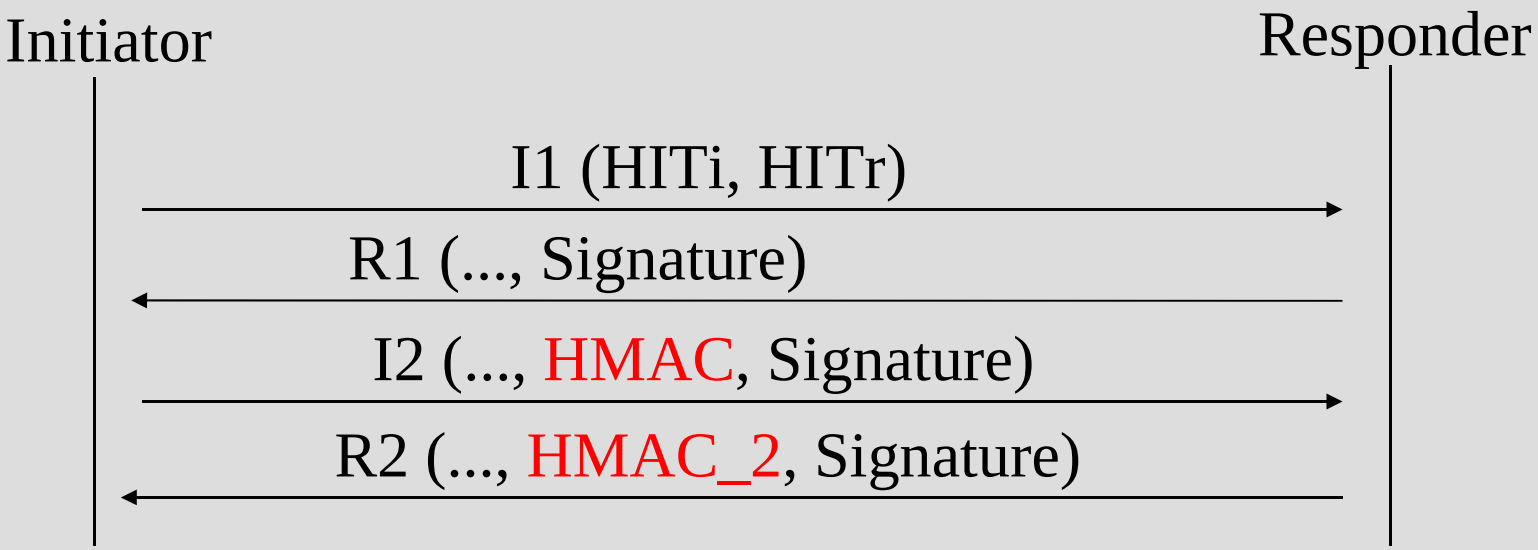
Closed issues

- Issue #46: 128-bit LSIs
  - Both 32-bit and 128 bit LSIs for IPv4 and IPv6 compatibility
  - 128-bit LSIs for resolving HIT/IPv6 collisions
  - LSI subnets still TBD
  - HITs changed to 128 bits (earlier 126 bits, with 2-bit prefix to separate them from IPv6 addresses)
- Issue #48: remove BOS and PAYLOAD packets
  - Bootstrapping and payload packets will be defined in separate drafts later
  - Not critical at this point

Closed issues (cont)

- Issue #39: Removal of HIP state
  - CLOSE / CLOSE ACK messages added
  - State machine: CLOSING, CLOSED added
- Issue #47: Make RSA mandatory algorithm
  - Changed the mandatory implementation from DSA to RSA
  - DSA is still recommended
- Transform algorithm change
  - Mandatory algorithm changed from 3DES to AES
  - (see Julien's e-mail: 22 Oct 04 Encryption Transform)

Make HIP SIGMA compliant



I2: New HMAC TLV covering the whole packet
R2: Changed HMAC, calculation covers also Responders HOST_ID

HMAC_2 TLV definition and calculation requires re-writing

Open issues

- Issue #31: LSI 1.0.0.0/8 allocation from IANA
  - Also 128-bit LSI prefix allocation
- Issue #37: Notification data field usage
  - Data field description for different parameters
- Issue #49: IANA considerations section
  - This section must be written
- Issue #50: Remove Appendix E
  - Running HIP over IPv4 UDP
- ... + a number of editorial things