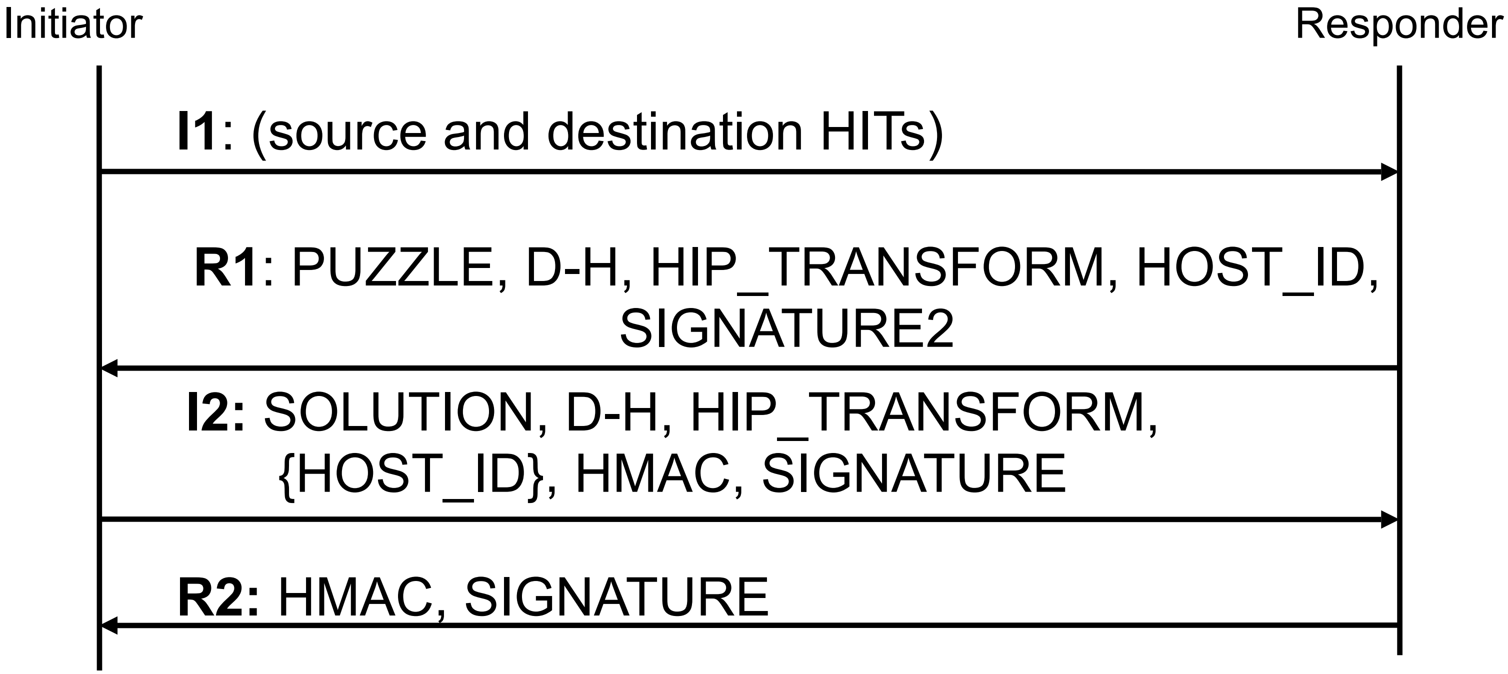
HIP base specification draft-ietf-hip-base-02

Petri Jokela and Pekka Nikander

The HIP base exchange


Initiator
Responder
I1: (source and destination HITs)
R1: PUZZLE, D-H, HIP_TRANSFORM, HOST_ID, SIGNATURE2
I2: SOLUTION, D-H, HIP_TRANSFORM, {HOST_ID}, HMAC, SIGNATURE
R2: HMAC, SIGNATURE

Base HIP: additional messages

- CER
- UPDATE
  - change connection parameters
  - usage defined in separate documents
- NOTIFY
  - provide fault information to the peer
- CLOSE – CLOSE_ACK

Changes between -01 and -02

- ESP transform usage moved to draft-jokela-hip-esp-00
  - Modular structure, enables new transforms
- A new restriction for HIT values
  - All HITs must begin with binary 01 or 10
  - The restriction to be lifted at January 1st 2009
- Appendix A (API) removed (issue 54)
- User data transmission format ”negotiation” (issue 55)
  - Type values 2048-4095 reserved for transforms
  - Parameters in preferred order, not in type order

Current open issues

- Issue 49: IANA considerations section
  - This section is missing
- Issue 53: Move LSIs into a separate draft; relatedly
- Issue 31: LSI 1.0.0.0/8 allocation from IANA
  - No actions taken yet

New open issues

- HIT formation with SHA-1
  - Use HMAC instead of plain hash?
  - Use SHA-256?
  - Update HIT length to 256 bits?
- Generalisations as proposed by Tom
  - A separate presentation
- Comments received from Tuomas Aura
  - To be handled on the mailing list

Next steps

- Resolve the new open issues at the mailing list
  - Generalisation
  - Comments from Tuomas Aura
- Update implementations?
- Working group last call by Paris?