Current status

Chairs

Status overview

- Architecture draft at the RFC Editor
  - To be published as an Informational RFC
- Base protocol specification closing completion
  - Resolving last open issues, based on interops
- Proposal for ESP extensions (BEET mode)
  - Complete draft; easier HIP implementation
- More work needed on infrastructure issues
  - Multi-addressing, DNS interactions, NAT traversal, rendezvous / proxy

Architecture specification

- draft-moskowitz-hip-arch-05.txt
- Submitted to the RFC Editor on Oct 27th
- Intended to be published as Informational
- Reasons for such early submission
  - Create a snapshot of current thinking
  - Create a starting point for the proposed WG

Base protocol specification

- draft-moskowitz-hip-08.txt
- First complete, fully specified version
- Open issues
  - Appendix containing packet examples
  - Exact bit formats for extension capability
  - Clarification on ESP SA key generation
  - Clarification on D-H key material generation
  - Small bug in state machine description

IPsec ESP extensions

- draft-nikander-esp-beet-mode-00.txt
  - Also discussed at ipsec wg and mobike bof
- Bound End-to-End Tunnel mode
- Transport mode processing with limited tunnel mode semantics
  - Fixed inner addresses, no address ranges
- Translates inner addresses (HITs) to outer addresses on output and back on input

Multi-addressing

- draft-nikander-hip-mm-00.txt
- Security analysis and protocol goals ok
- Proposed solution needs to be reworked
  - Needs better SA handling to take care of different QoS properties of different paths
  - Packet formats must be updated to match the newly added extension capability

DNS interactions

- No drafts yet
- Need a method to store HIs or HITs
- Minimum level: Store HIT in an AAAA like RR
- Better: Store HI in an IPSECKEY like RR
- Maybe: DNS updates secured with HIP

NAT traversal

- No drafts yet
- Work must be aligned with multi-addressing
- Basic idea: Let NATs learn SPIs from HIP messages, setting up SPI based NAT (SPINAT)

Rendezvous / proxy server

- No drafts yet
- Rendezvous server allows fast / simultaneous mobility
  - Dynamic DNS updates are not fast enough
- Proxy allows a HIP host to use multi-addressing when communicating with a non-HIP host
- Functionality fairly similar; a proxy can easily function as a rendezvous server, too