Generalizing the HIP base protocol (draft-henderson-hip-generalize-00.txt)

March 9, 2005

Tom Henderson

Executive summary

- A few small changes to the base protocol now may give us more room to experiment in the future

1. Generalize HIT fields to “upper layer identifier (ULID)”
2. Allow multiple usage profiles for HIP handshake
3. Do not mandate that specific HIP messages carry specific parameters

Motivation

- Should we be allowing for more experimentation in the use of HIP protocols?
  - HIP protocols perceived to be too inflexible by some
  - Find the common ground between a number of similar proposals, and see how HIP fits

HIP mobile IP shim6 i3 NIMROD

IPNL DataRouter TRIAD FARA

Network Pointers DOA SIM MAST/CELP

SCTP WIMP MOBIKE Hi3

Generalized architecture

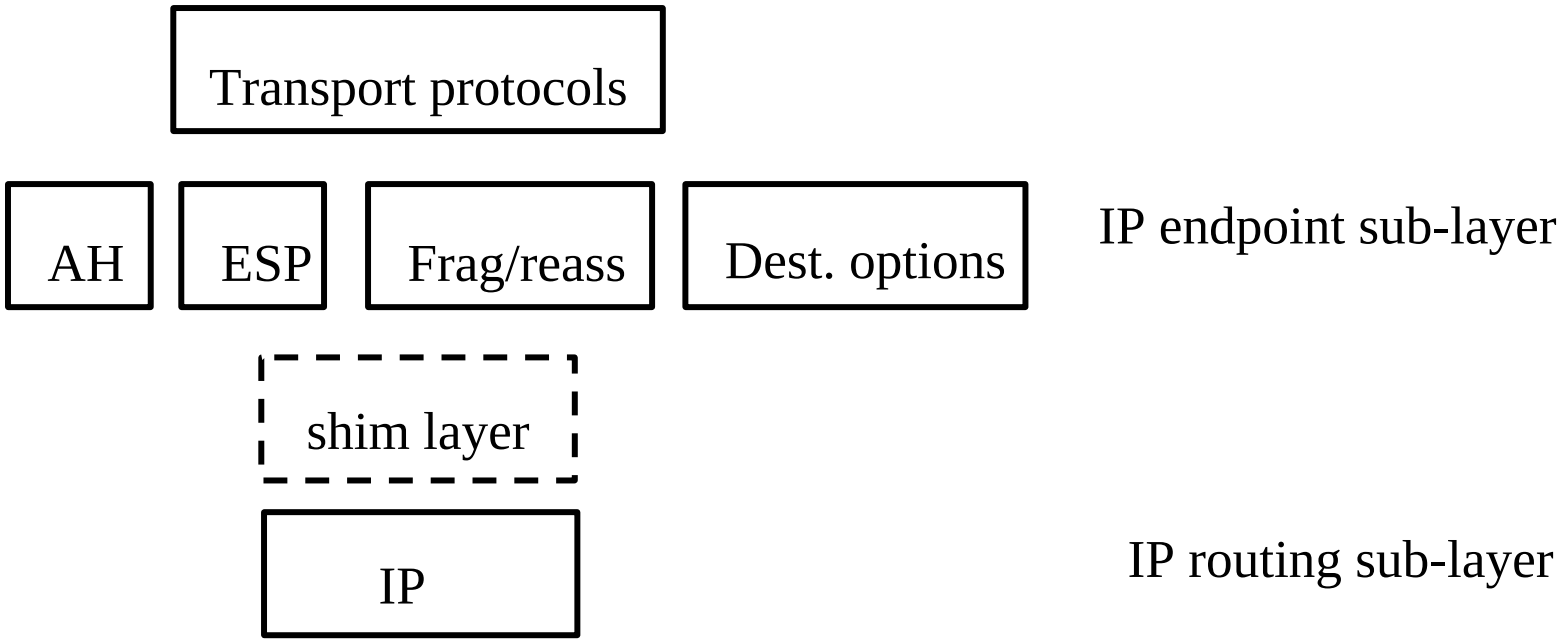

Figure adapted from:
E. Nordmark and M. Bagnulo, “Multihoming L3 Shim Approach,” draft-ietf-multi6-l3shim-00, January 2005

Decomposition

1. Upper-layer identifier: HIT, but also mobile IP home address, unique-local address, identifier-address, and other identifiers at other layers (e.g., session)
2. Address resolution: "Early binding" (HIP) or "late binding" (e.g., i3, mobile IP through home agent)
3. Context establishment: HIP handshake, but also IKE/MOBIKE and shim6
4. Per-packet context: SPI, but also Routing Headers/Destination Options, or explicit shim headers
5. Locator management: HIP mobility/multihoming, but also MAST, CELP, multi6 locator selection, hash-based addresses

Combinations

- HIP/i3 (Hi3)
- HIP/IKE (or MOBIKE)
- HIP/mobile IP
- HIP/multi6
- HIP rendezvous server and STUN

Would a generalized protocol make these combinations easier?

Proposal 1. Identifiers

- Allow use of non-HIT identifiers (or non-128 bit identifiers)
  - Used as ULIDs in transport protocol
  - Pekka has suggested a few standard sizes rather than TLV format (e.g. 32, 64, 128, 256, 512)
- Benefits:
  - Future evolutions in HITs (e.g., current SHA-1 concerns)
  - More flexibility in invoking HIP handshake
    - What if context establishment is deferred, and IP addresses used in transport sockets?

Proposal 2. Handshake types

- Allow use of handshake variants
  - Existing handshake would be one usage profile
    - SIGMA-compliant DH key exchange
  - Perhaps indicated as different flavors of I1, or a type parameter
- Benefits
  - Allowing lighter-weight handshakes such as WIMP (based on hash chains)

Proposal 3. Mandatory parameters

- Do not mandate that packet types carry mandatory parameters
  - Only mandatory parameters are the identifiers (was the HITs)
  - Handshake type defines the usage profile (requirements) on later messages
  - e.g. if I1 indicates current HIP usage profile, then R1 MUST include PUZZLE
- Corollary: avoid making statements such as ESP is a “MUST” implement
- This mainly affects how draft is organized and written

Security considerations

- Mixing and matching of protocol elements obviously changes the security properties
  - Leave this for other drafts
- May offer a more gradual path forward to a HIP-enabled world (with better security)

Summary

- Current HIP could be defined as a “usage profile” of a slightly more generalized protocol
- Possible benefits:
  - HIP elements could be considered for the shim6 protocol
  - HIP messaging may be able to secure mobile IPv6 Binding Update
  - Might allow other identifier types while still enabling the ID/locator separation