Host Identity Protocol (HIP): Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6

by Pekka Nikander, Andrei Gurtov, and Thomas R. Henderson

Johannes Bachhuber

Jacobs University Bremen

j.bachhuber@jacobs-university.de

March 26, 2014

Overview

Introduction

- What is the Host Identity Protocol?
  - Internetworking architecture and associated set of protocols
  - Developed by the IETF HIP Working Group
- Additional namespace between transport and network layer
  - Cryptographic host identifiers replace IP addresses in transport layer
- Backwards compatibility
  - No changes needed in applications and routers
- Simplification of previously hard networking problems
  - Mobility and Multi-Homing through separation of identity and location
  - Integrated end-to-end security
  - Privacy and accountability

Problem Statement - Evolving Environments

- When TCP/IP was designed, requirements were different
  - End users were considered mutually trusting
  - Network was assumed to be unreliable
- Of the four classical network-layer invariants, all but reversibility have been violated
  1. **Non-mutability:** source and destination identifiers sent = identifiers received
  2. **Location independence:** identities don't change during a connection
  3. **Reversibility:** Reversing direction by reversing source and destination identifiers
  4. **Omnisciency:** Host knows its own identities

Problem Statement - Evolving Environments

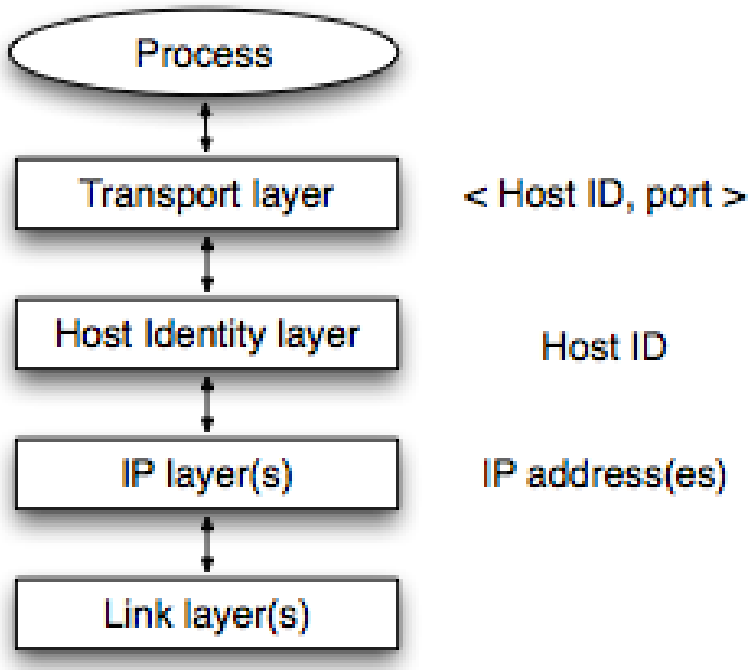
- Modern networks have a different set of requirements:
  1. Independence from underlying network
  2. Surviving in (partially) hostile environment, where co-operation between networks is limited
  3. Native support for mobility and multi-access
  4. Location privacy to network and third parties
- There is also a set of new problems, that weren't thought of initially
  - Loss of universal connectivity
  - Problems with multicast
  - Unwanted traffic
  - Need for encryption and authentification support

Architecture - Overview

- Implementation of identifier / locator split approach
- New Host Identity (HI) namespace, located between IP and DNS namespaces
  - Restores the classic four invariants in the new HI namespace
  - Allows for flexible, location based IP namespace
- Host Identity is the public key from a public-private key-pair
  - Host has ownership of private key $\rightarrow$ can prove its identity

Architecture - Stack

- On the layers above the HIP layer, the IP address (locator) need not be known
- Host Identity Tag (HIT) or Local Scope Identifier (LSI) used instead
- HIP is used to transfer IP changes without an application's knowledge



Architecture - HITs and LSIs

Host Identity Tags (HITs) - IPv6

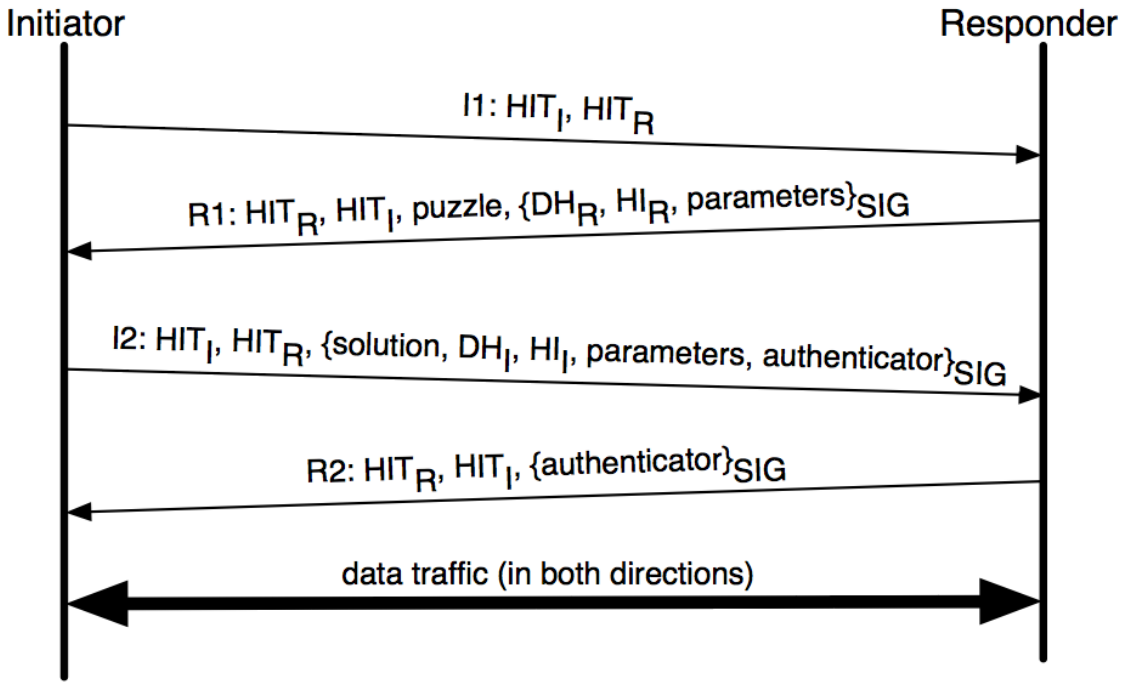
- 128 bit representation of the Host Identity's public key
- 28 bit prefix 2001:0010::/28 (called Orchids)
- 100 bits cryptographic hash of the public key
- HIT provides a IPv6 look-alike shorthand, whose origin from a Host Identity can easily be verified

Local Scope Identifiers (LSIs) - IPv4

- 32 bit representation of the Host Identity's public key
- IPv4 addresses are too short to guarantee global uniqueness
- Only assumed to be locally unique
- Not sent on the wire within HIP

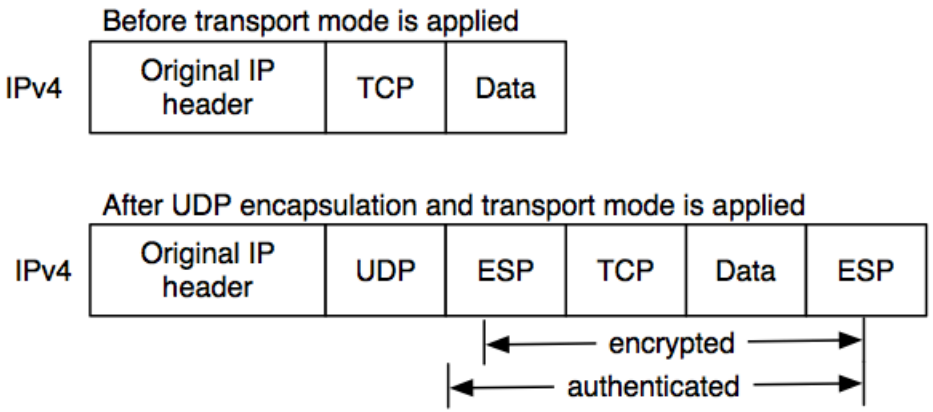
Architecture - Connection Initialization

- 4-way handshake (Base Exchange)
- R1 is simply triggered by I1
- No responder state after R1
- Puzzle protects from SYN-flodding like attacks
- After I2, R is confident of I's identity
- If desired, R establishes the connection with R2



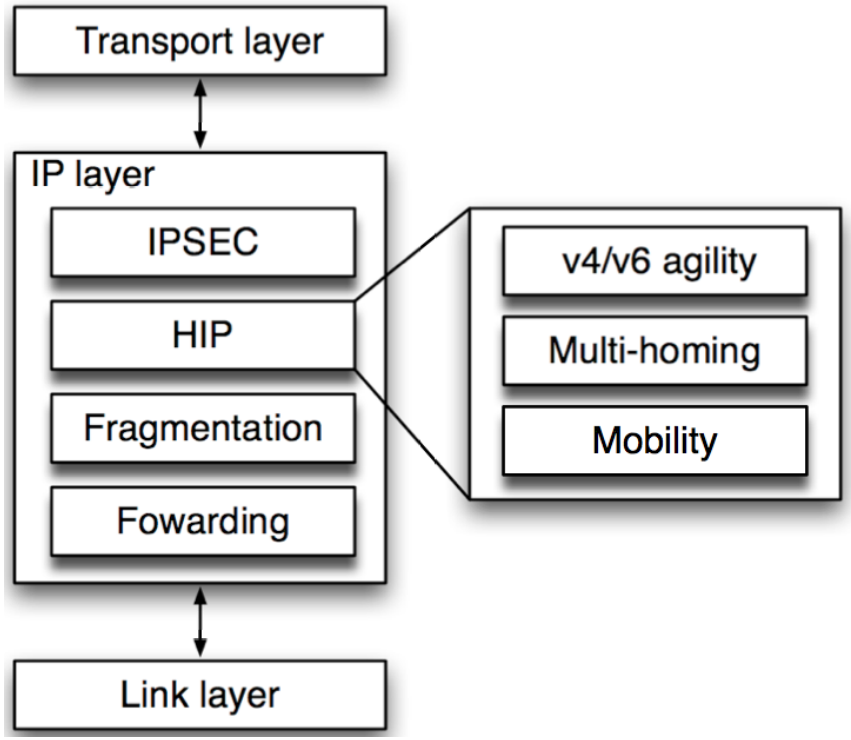
Architecture - NAT Traversal

- Default: HIP carried in IP packets
- Large number of IPv4 NATs don't pass traffic with this protocol number
  - Possibility of carrying HIP control messages in UDP packets
- RFC 5770 has since been published with exact specifications



Architecture - Detailed Layering

- HIP splits IP layer into routing related and end-to-end related functionalities
- IPsec is above HIP, although in practise HIP is often embedded in IPsec SA processing



Features - Multi-Homing and Mobility

- Source IP addresses irrelevant, as long as return address is known
- HIP mobility and multi-homing extension defines locator parameter containing the sender's IP address(es)
  - When a host changes its IP, a HIP control packet with the new IP(s) is sent to all (active) peer hosts
  - Reachability needs to be verified
  - Multiple IPs can be mixed IPv6 and IPv4 addresses
- Rendevouz servers keep track of hosts IPs and forward the first HIP control message (I1 from Handshake)
  - Similar to MobileIP, but only a single control message needs to be forwarded
  - Any HIP host could act as rendevouz server, but static servers need to be present too
- Make-before-break handovers supported to avoid packet loss

Features - Multi-Homing and Mobility cont'd

- Subnet mobility through delegation
  - Delegating rights is easily achieved through cryptographic signing with the HIP private key
  - HIP control messages containing locators can be sent be routers
- Application-level mobility
  - Service instances can be allocated a HIT, which receive delegated rights to act on behalf of service
  - Physical location mobile through delegation to host system

Features - Security

- HIP provides a number of security improvements over traditional TCP/IP
- Accountability is improved through the use of cryptographic keys as Host Identifiers
- Privacy can still be achieved in several ways
  - Host Identifiers are self-generated, not given out like IP addresses
  - Multiple HIs can be used
  - Even further improved privacy through BLINK extention
- End-to-end encryption is provided through IPSec
- Unwanted traffic and DDoS attacks can be avoided more easily
  - 4-way handshake with no recipient state after first response prevents SYN-flood
  - Puzzle sent with R1 can have varying complexity - it's possible to adjust this on the fly as loads change

Challenges

- Managing new HIP name space
  - HIP names have no inherent structure, unlike IPs, DNS names, etc
  - Trust that you get the right HIT needs to be established
  - DNSSEC, SPKI/SDSI, X509 Certificates
- Delays caused by handshake: solving puzzle, key exchange
- Third party referral problem
- IPsec over IPsec - not specified
- Legacy, HIP-unaware NATs

Maturity - Standardization

- HIP is still on the experimental track, although the paper talked about the possibility of moving to the standardization track soon
- A variety of HIP related RFCs have been published by the HIP WG
  - Most RFCs are from 2008, this paper was written early 2009
  - It has been relatively quiet since 2011 (5 RFCs in 2011)
  - New RFC (RFC 7086) on HIP BONE and RELOAD published this January
  - Quite a few internet drafts from 2013 around
- According to the paper 2 EU governments were considering adopting HIP in early 2009, although I could not find any evidence of it actually being adopted

Maturity - Implemtations and Usage

- The required kernel modifications are included in Linux starting with version 2.6.21
- I could not find evidence of wide-spread usage
- OpenHIP is curently at version 0.9, published in early 2012

References

Pekka Nikander, Andrei Gurtov, and Thomas R. Henderson (2010)

Host Identity Protocol (HIP): Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6 Networks

IEEE COMMUNICATIONS SURVEYS & TUTORIALS 12(2), 186 – 204.

IETF HIP Working Group

`http://datatracker.ietf.org/wg/hip/` Accessed on March 25, 2014.

OpenHIP website

`http://www.openhip.org/` Accessed on March 25, 2014.

RFQ, RFC, and RFF

Request for Question/Request for Comments/Request for Feedback

The End