Host Identity Protocol

Pekka Nikander
Ericsson Research Nomadiclab and
Helsinki Institute for Information Technology
http://www.hip4inter.net

Presentation outline

- Introduction: What and why?
- Background
- HIP in a Nutshell
- Mobility and multi-homing (multi-addressing)
- HIP infrastructure: Hi^3
- Current status
- Summary

What is HIP?

- HIP = Host Identity Protocol
- A proposal to separate identifier from locator at the network layer of the TCP/IP stack
- A new name space of public keys
- A protocol for discovering and authenticating bindings between public keys and IP addresses
- Secured using signatures and keyed hashes (hash in combination with a secret key)

Motivation

- Not to standardise a solution to a problem
  - No explicit problem statement
- Exploring the consequences of the id / loc split
  - Try it out in real life, in the live Internet
- A different look at many problems
  - Mobility, multi-homing, end-to-end security, signalling, control/data plane separation, rendezvous, NAT traversal, firewall security, ...

Presentation outline

- Introduction: What and why?
- Background
- HIP in a Nutshell
- Mobility and multi-homing (multi-addressing)
- HIP infrastructure: Hi^3
- Current status
- Summary

Background

- A brief history of HIP
- Architectural background
- Related IETF Working Groups

A Brief History of HIP

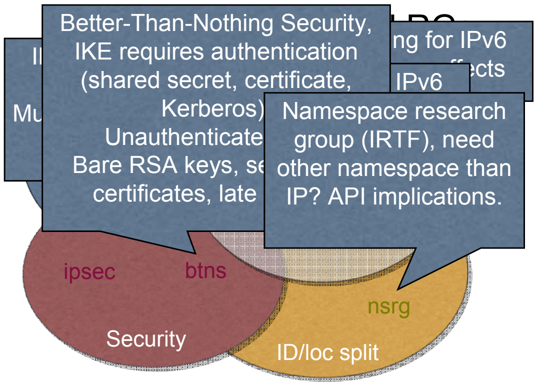
- 1999 : idea discussed briefly at the IETF
- 2001: two BoFs, no WG created at that time
- 02-03: development at the corridors
- 2004: WG and RG created
- Now: base protocol more or less ready
  - Four interoperating implementations
- More work needed on mobility, multi-homing, NAT traversal, infrastructure, and other issues

Architectural background

- IP addresses serve the dual role of being
  - End-point Identifiers
    - Names of network interfaces on hosts
  - Locators
    - Names of naming topological locations
- This duality makes many things hard

New requirements to Internet Addressing

- Mobile hosts
  - Need to change IP address dynamically
- Multi-interface hosts
  - Have multiple independent addresses
- Mobile, multi-interface hosts most challenging
  - Multiple, dynamically changing addresses
- More complex environment
  - e.g. local-only connectivity



Better-Than-Nothing Security, IKE requires authentication (shared secret, certificate, Kerberos) Unauthenticate Bare RSA keys, se certificates, late

ng for IPv6 ects

IPv6

Namespace research group (IRTF), need other namespace than IP? API implications.

Presentation outline

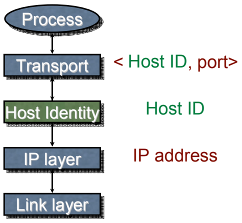
- Introduction: What and why?
- Background
- HIP in a Nutshell
- Mobility and multi-homing (multi-addressing)
- HIP infrastructure: Hi^3
- Current status
- Summary

HIP in a Nutshell

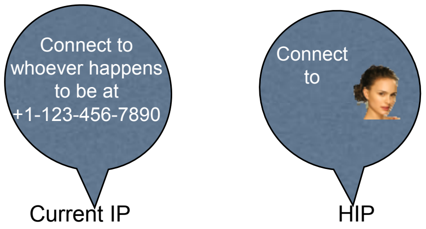
- Architectural change to TCP/IP structure
- Integrates security, mobility, and multi-homing
  - Opportunistic host-to-host IPsec ESP
  - End-host mobility, across IPv4 and IPv6
  - End-host multi-address multi-homing, IPv4/v6
  - IPv4 / v6 interoperability for apps
- A new layer between IP and transport
  - Introduces cryptographic Host Identifiers

The Idea

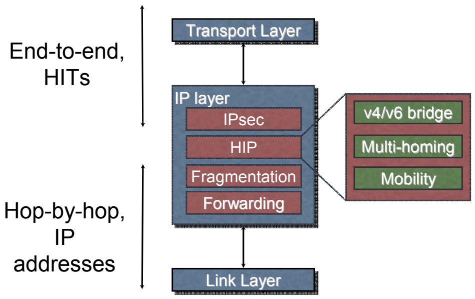
- A new Name Space of Host Identifiers (HI)
  - Public crypto keys!
  - Presented as 128-bit long hash values, Host ID Tags (HIT)
- Sockets bound to HIs, not to IP addresses
- HIs translated to IP addresses in the kernel



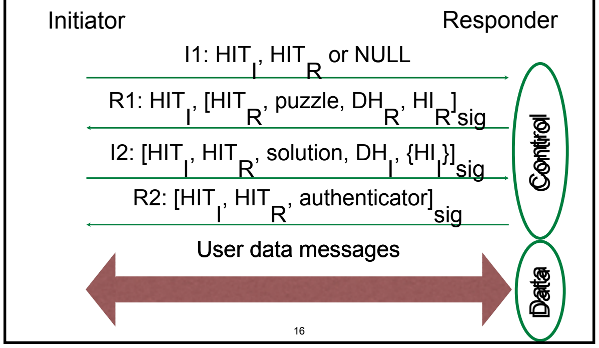
An analogy: What if people were hosts



More detailed layering



Protocol overview



I1: HIT_I, HIT_R or NULL

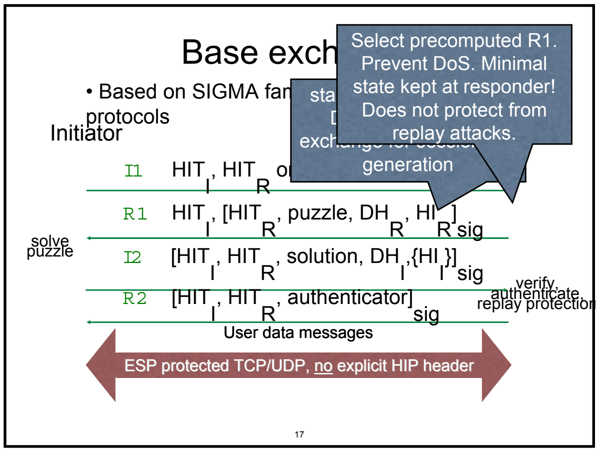
R1: HIT_I, $[\mathrm{HIT}_R$, puzzle, DH_R, $\mathrm{HI}_R]_{sig}$

I2: $[\mathrm{HIT}_I$, HIT_R, solution, DH_I, $\{\mathrm{HI}_I\}]_{sig}$

R2: $[\mathrm{HIT}_I$, HIT_R, authenticator$]_{sig}$

Base exch

- Based on SIGMA fan protocols


Initiator
solve puzzle
verify, authenticate, replay protection
User data messages
ESP protected TCP/UDP, no explicit HIP header

I1 HIT_I, HIT_R or

R1 HIT_I, $[\mathrm{HIT}_R$, puzzle, DH_R, $\mathrm{HI}_R]_{sig}$

I2 $[\mathrm{HIT}_I$, HIT_R, solution, DH_I,$\{\mathrm{HI}_I\}]_{sig}$

R2 $[\mathrm{HIT}_I$, HIT_R, authenticator$]_{sig}$

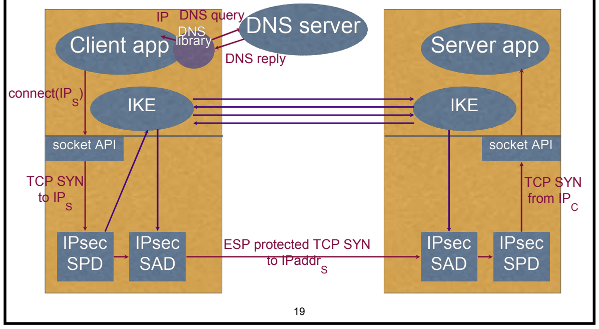
sta [exchange for session generation

Select precomputed R1. Prevent DoS. Minimal state kept at responder! Does not protect from replay attacks.

Other core components

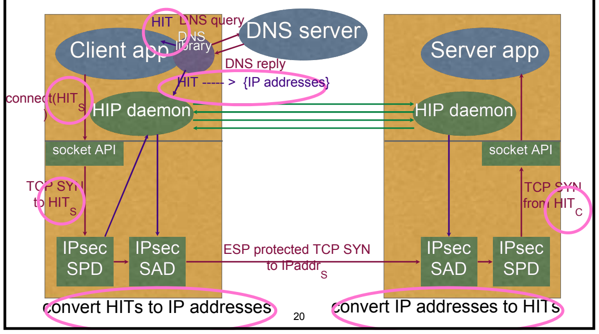
- Per-packet identity context
  - Indirectly, through SPI if ESP is used
  - Directly, e.g., through an explicit shim header
- A mechanism for resolving identities to addresses
  - DNS-based, if FQDNs used by applications
  - Or distributed hash tables (DHTs) based

How applications work today (when IPsec ESP is used)



19

One way to implement HIP

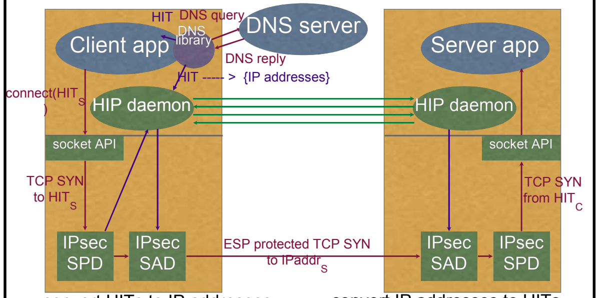


convert HITs to IP addresses

convert IP addresses to HITs

20

Using HIP with ESP



convert HITs to IP addresses

convert IP addresses to HITs

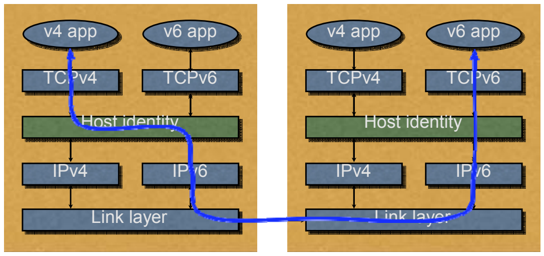
21

Many faces

- More established views:
  - A different IKE for simplified end-to-end ESP
  - Super Mobile IP with v4/v6 interoperability and dynamic home agents
  - A host multi-homing solution
- Newer views:
  - New waist of IP stack; universal connectivity
  - Secure carrier for signalling protocols

22

HIP as the new waist of TCP/IP



23

HIP for universal connectivity

- Goal:
  - Lowest layer providing location-independent identifiers and end-to-end connectivity
- Work in progress:
  - Support for traversing legacy NATs
  - Firewall registration and authentication
  - Architected middleboxes or layer 3.5 routing
  - Identity-based connectivity with DHTs

24

Signalling carrier

- Originally HIP supported only ESP-based user data transport (previous slides)
- ESP is now being split from the base protocol
- Base protocol is becoming a secure carrier for any kinds of signalling
- Support for separate signalling and data paths
  - Implicitly present in the original design
  - Now being made more explicit

Faces summary: Motivating architectural factors

- A “reachability” solution across NATs
  - New “waist” for the protocol stack
- Built-in security
  - Implicit channel bindings
    - `connect(HIT)` provides a secured connection to the identified host
  - Puzzle-based DoS protection
- Integrated mobility and end-host multi-homing

Presentation outline

- Introduction: What and why?
- Background
- HIP in a Nutshell
- Mobility and multi-homing (multi-addressing)
- HIP infrastructure: Hi^3
- Current status
- Summary

Introduction to IP based mobility and multi-homing

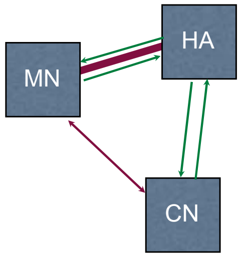
- Mobility implemented at “IP layer”
- IP addresses are assigned according to topology
  - Allows for routing prefix aggregation
- Mobile hosts change their topological location
- Multi-homed hosts present at many locations
- In an IP based m&m solution
  - Transport & apps do not see address changes or multiple addresses

Rendezvous

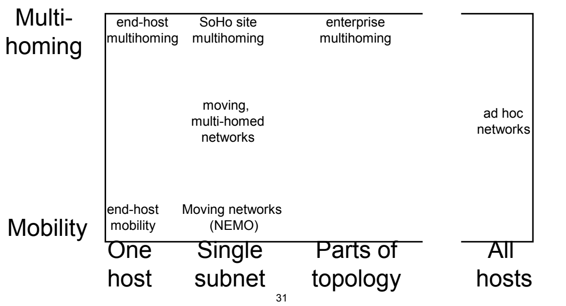
- Initial rendezvous
  - How to find a moving end-point?
  - Can be based on directories
  - Requires fast directory updates
    - →Bad match for DNS
- Tackling double-jump
  - What if both hosts move at same time?
  - Requires rendezvous point

Mobile IP

- Home Agent (HA)
  - Serves a Home Address
  - Initial reachability
  - Triangular routing
- Route optimization
  - Tunnels to bypass HA
  - HA as rendezvous point



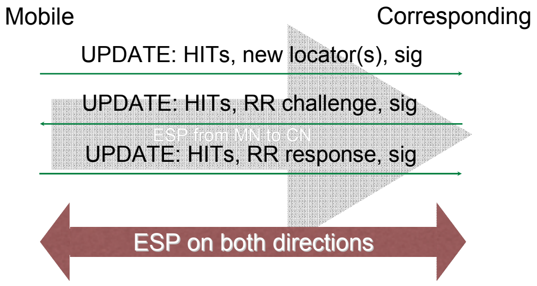
Multi-addressing dimensions



HIP Mobility & Multi-homing

- Mobility and multi-homing become duals of each other
  - Mobile host has many addresses over time
  - Multi-homed host has many addresses at the same time
- Leads to a Virtual Interface Model
  - A host may have real and virtual interfaces
  - Merges the “Home Agent”

Mobility protocol

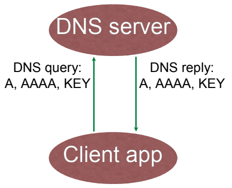

Mobile
Corresponding
UPDATE: HITs, new locator(s), sig
UPDATE: HITs, RR challenge, sig
ESP from MN to CN
UPDATE: HITs, RR response, sig
ESP on both directions

Presentation outline

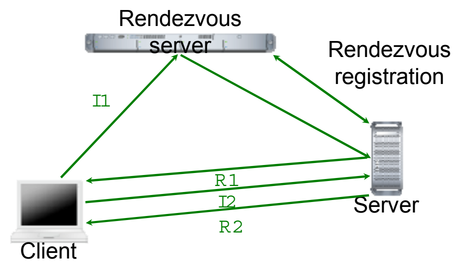
- Introduction: What and why?
- Background
- HIP in a Nutshell
- Mobility and multi-homing (multi-addressing)
- HIP infrastructure: Hi^3
- Current status
- Summary

Key distribution for HIP

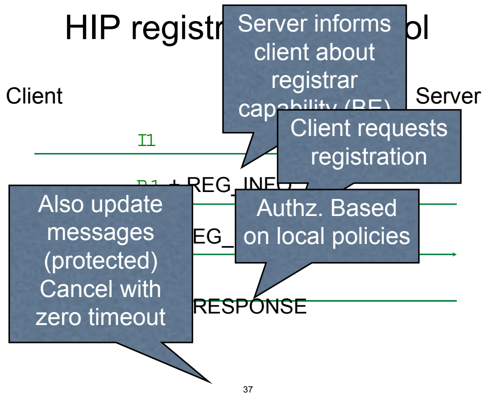
- Depends on application
- For multi-addressing, self-generated keys
- Usually keys in the DNS
- Can use PKI if needed
- Opportunistic mode supported
  - SSH-like leap-of-faith
  - Accept a new key if it matches a fingerprint



Basic HIP rendezvous



HIP registr ol



Server informs client about registrar capability (RE)

Client requests registration

Also update messages (protected) Cancel with zero timeout

Authz. Based on local policies

The infrastructure question

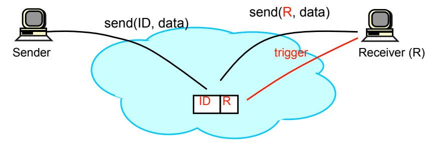
- HIs originally planned to be stored in the DNS
  - Retrieved simultaneously with IP addresses
  - Does not work if you have only a HIT
- Question: How to get data based on HIT only?
  - HITs look like 128-bit random numbers
- Possible answer: DHT based overlay like i^3

Distributed Hash Tables

- Distributed directory for flat data
- Several different ways to implement
- Each server maintains a partial map
- Overlay addresses to direct to the right server
- Resilience through parallel, unrelated mappings
- Used to create overlay networks

i^3 rendezvous abstraction

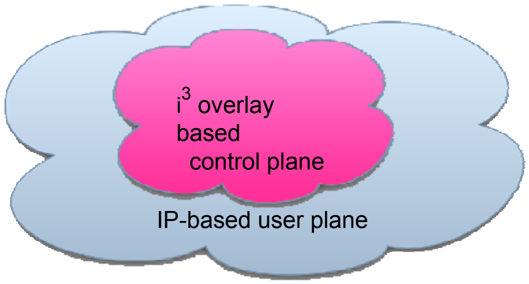
- Trigger inserted by receiver(s)
- Packets addressed to identifiers
- i^3 routes packet to the receiver(s)



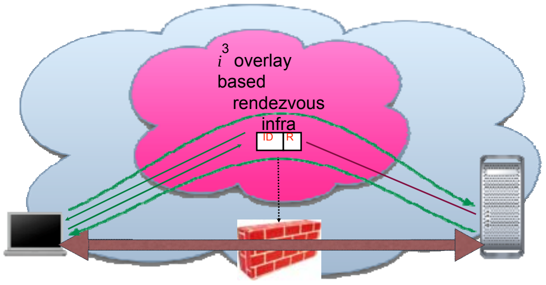
Hi^3: combining HIP and i3

- Developed at Ericsson Research IP Networks
- Uses i^3 overlay for HIP *control* packets
  - Provides rendezvous for HIP
- *Data* packets use plain old IP
  - Cryptographically protected with ESP
- Only soft or optional state in the network

$\text{H}i^3$ and DHT-based rendezvous



Control/data separation



Hi^3 overlay and IPsec connectivity

- i^3 overlay for signalling (control plane)
  - Routes only HIP control packets
- e2e ESP for data traffic (user plane)
  - Firewalls/middle boxes opened dynamically
- Only end-to-end signalling (HIP)
  - Middle boxes “snoop” e2e messages
- Lots of details to be filled in

An Internet control plane?

- HIP separates control and data traffic
- Hi^3 routes control traffic through overlay
  - Control and data packets take potentially very different paths
- *Allows* telecom-like control …
  - … but does not *require* it

Benefits for everyone

- Operators
  - Control, security, resilience, revenue
- Enterprises
  - Security, resilience, mobility
- Individual users
  - Security, mobility, ease of use

Benefits to operators

- More controlled network
  - Data requires HIP handshake first
- Protection against DoS and DDoS
- Resilience
  - Integrated multi-homing
  - No single points of failure

Benefits to enterprises

- More secure firewalls
- Integrated mobility and multi-access
  - Across IPv4 and IPv6
  - No single points of failure

Benefits to users

- DoS and DDoS protection
- Supports home servers (NAT traversal)
- Configuration free baseline security (ssh-like leap-of-faith encryption

Presentation outline

- Introduction: What and why?
- Background
- HIP in a Nutshell
- Mobility and multi-homing (multi-addressing)
- HIP infrastructure: Hi^3
- Current status
- Summary

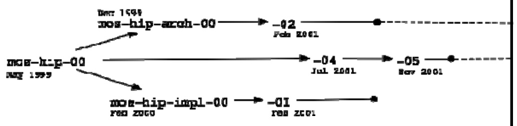
Current status

- WG and RG formed at the IETF / IRTF
  - First meetings in Seoul, March 2004
- Four known interoperating implementations
- A number of internet drafts
- Base specifications start to be mature
- About a dozen papers published or submitted

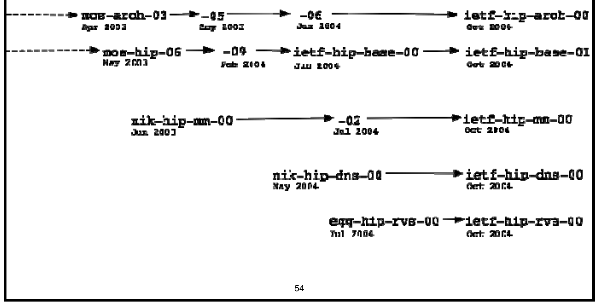
Implementation status

- Four interoperating implementations
  - Ericsson Research Nomadiclab, FreeBSD
  - Helsinki Institute for Information Tech., Linux
  - Boeing Phantom Works, Linux and Windows
  - Sun Labs Grenoble, Solaris
- Other implementations
  - Indranet (obsolete), DoCoMo US Labs, rumours about other

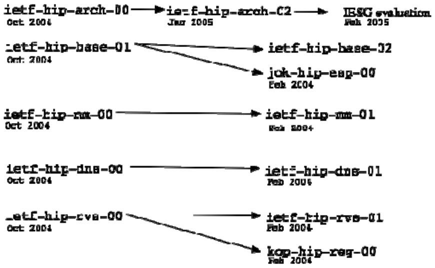
Evolution of drafts: Early era



Evolution of drafts: Restart



Evolution of drafts: 2005



Architecture

Base exchange

Mobility & multi-homing

DNS

Rendezvous

Registration

Current status

- RFCs
  - Host Identity Protocol (HIP) Architecture RFC 4423
- RFC queue
  - Host Identity Protocol (HIP) Domain Name System (DNS) Extensions
- IESG Processing
  - Host Identity Protocol
  - End-Host Mobility and Multihoming with the Host Identity Protocol
  - Host Identity Protocol (HIP) Rendezvous Extension
  - Host Identity Protocol (HIP) Registration Extension
  - Using ESP transport format with HIP
  - Using the Host Identity Protocol with Legacy Applications
- Internet-Drafts
  - HIP Extensions for the Traversal of Network Address Translators
  - Native Application Programming Interfaces for SHIM APIs

Summary

- New cryptographic name space
  - IP hosts identified with public keys
- Integrates security, mobility, multi-homing
- Evolving into a more generic signalling carrier
- Four interoperating implementations (total 7?)
- Base specifications start to be mature
- `http://www.hip4inter.net`
- `http://www.tml.hut.fi/~pnr/publications/`