Host Identity Protocol its potential relevance to Grids

Andrei Gurtov

Helsinki Institute for Information Technology

KnowARC

8.11.2006

(HIP slides thanks to Pekka Nikander/Nomadic Lab)

Outline

- Host Identity Protocol overview
- Snapshot on InfraHIP project
- Snapshot on NordicHIP project
- What can HIP offer for Grids?
- Snapshot on NI HAO Grid project

Architectural background

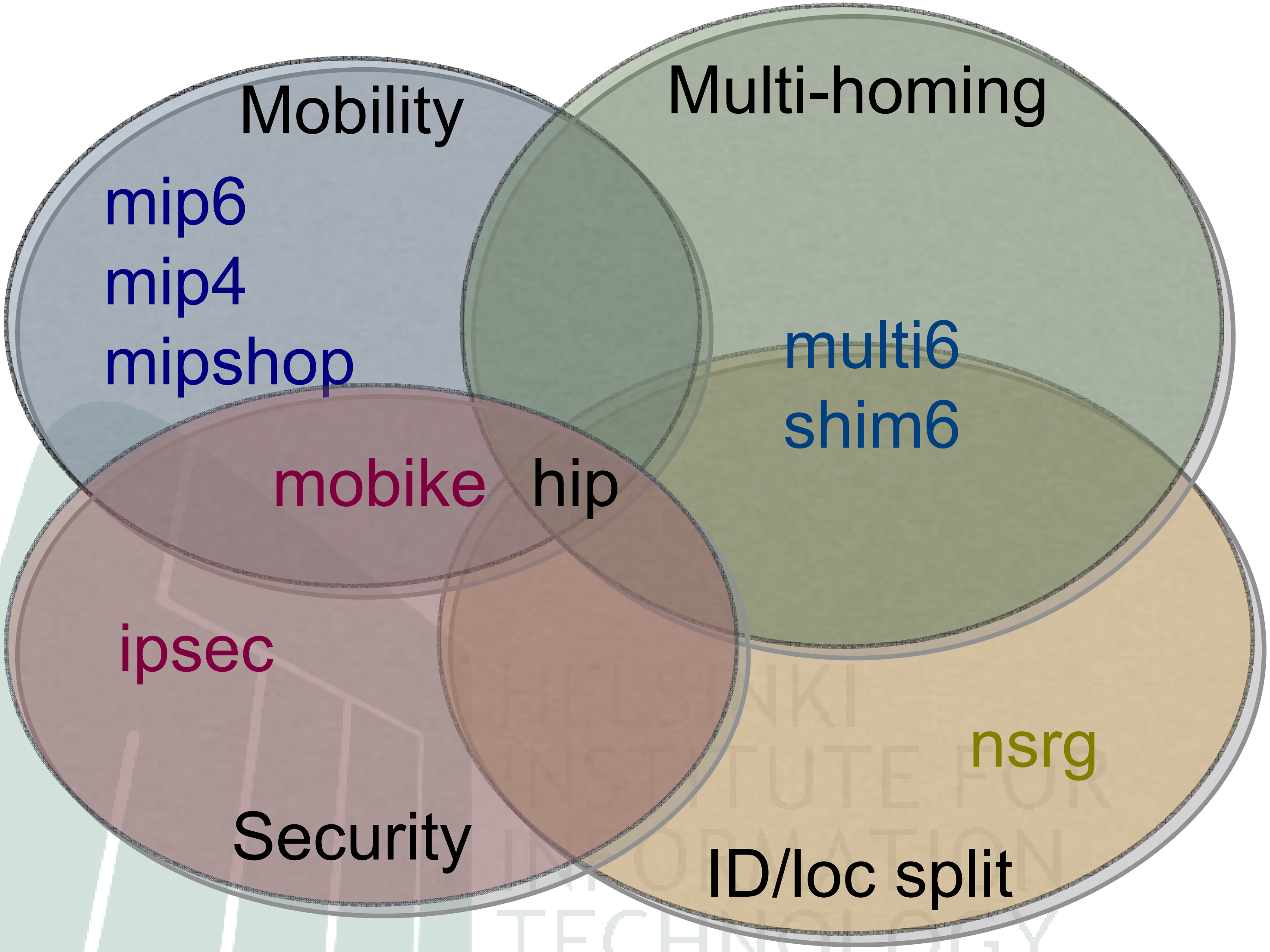
- IP addresses serve the dual role of being
  - End-point Identifiers
    - Names of network interfaces on hosts
  - Locators
    - Names of naming topological locations

- 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

Related IETF WGs and RGs



Mobility

mip6
mip4
mipshop

Multi-homing

multi6
shim6

mobike

hip

ipsec

Security

nsrg

ID/loc split

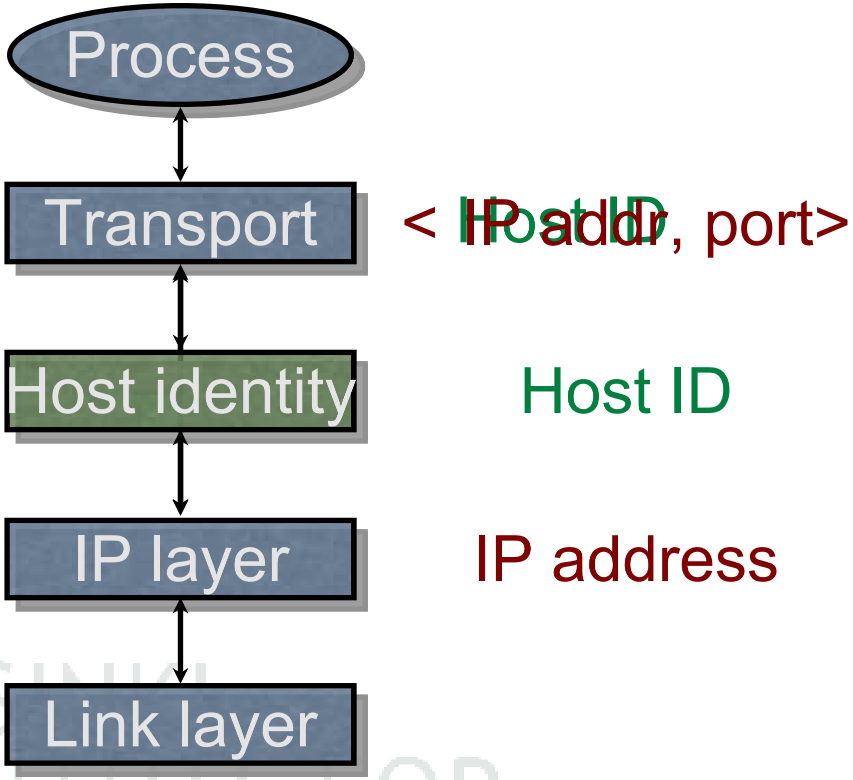
HIP in a Nutshell

- 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

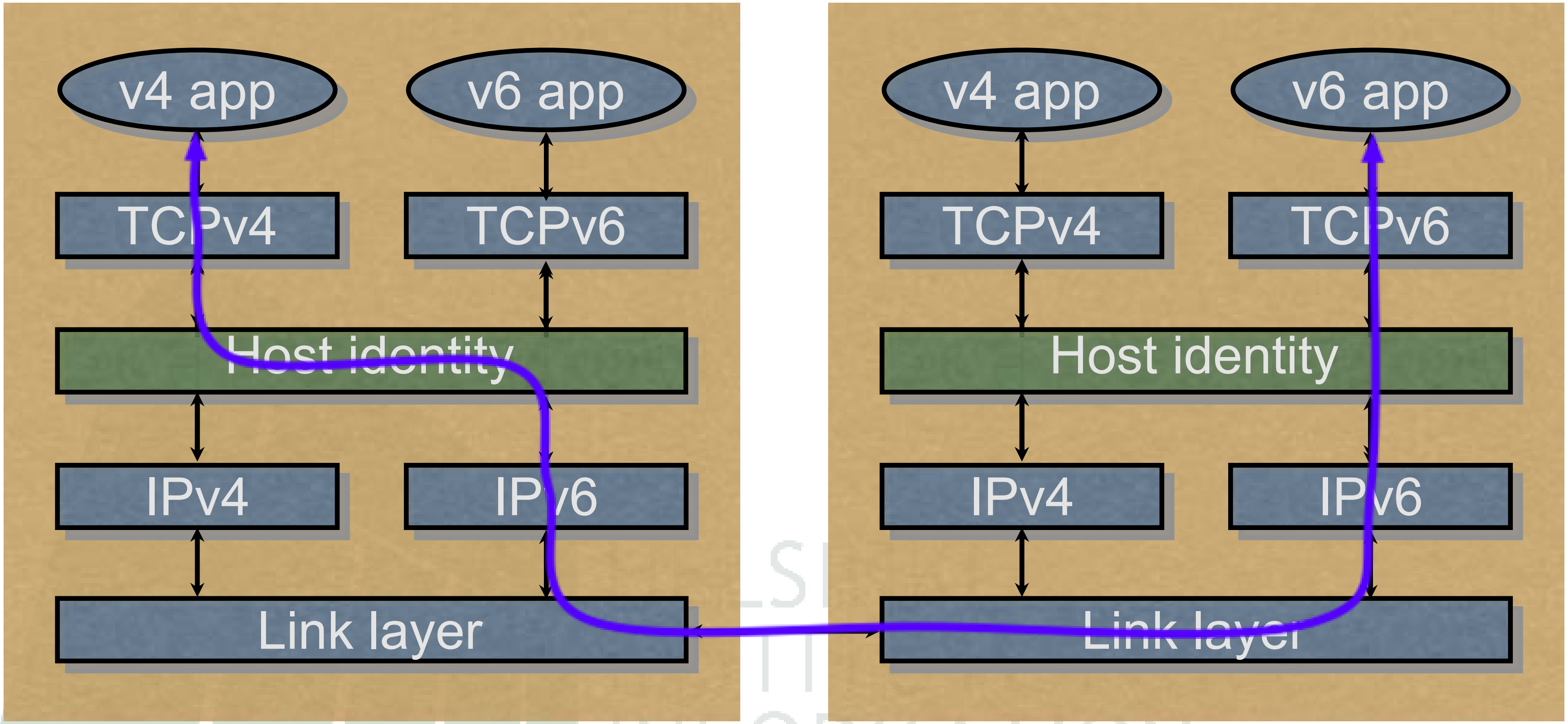
The Idea

- A new Name Space of Host Identifiers (HI)
  - Public crypto keys!
  - Presented as 128-bit long hash values,

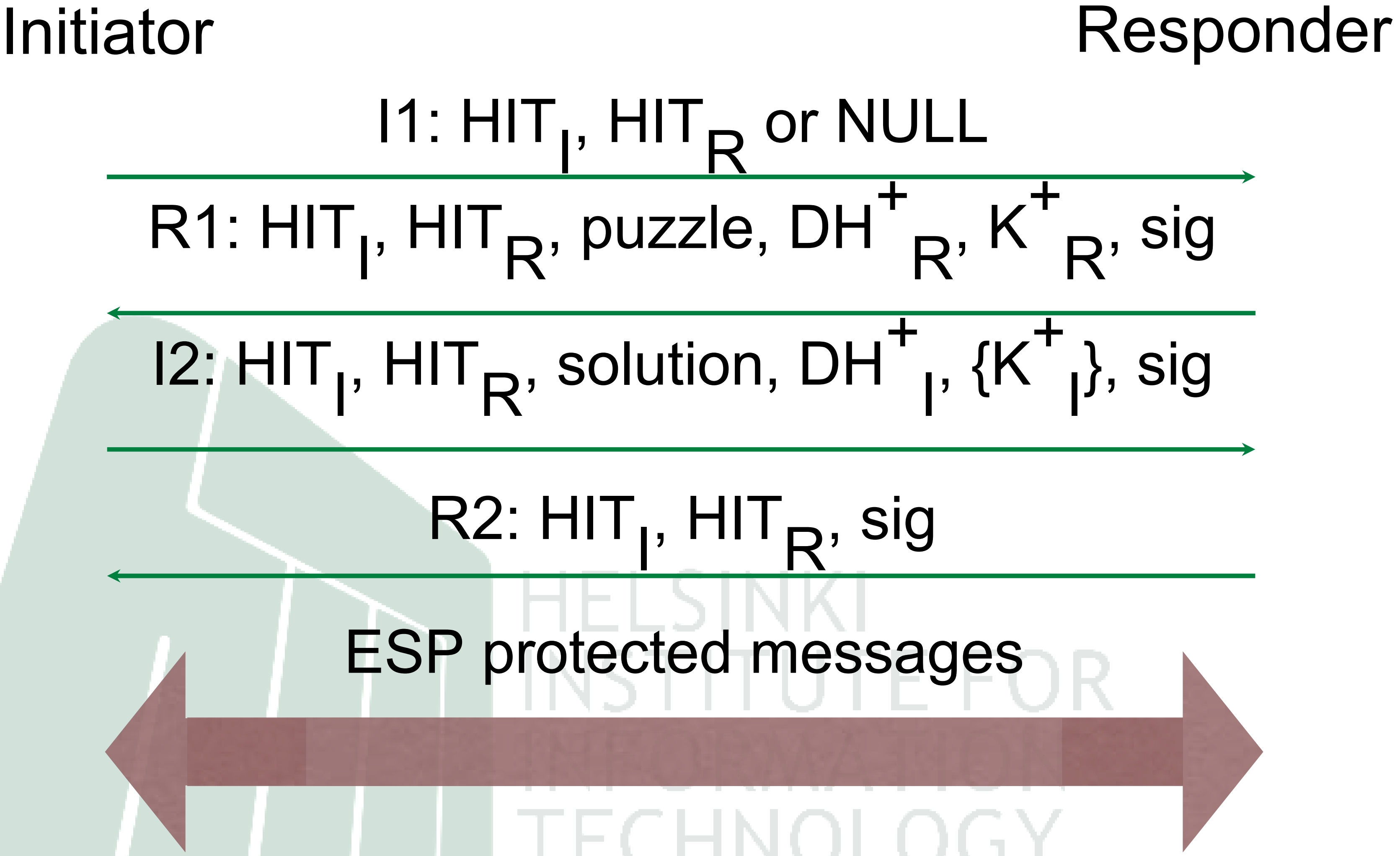
  Host ID Tags (HIT)
- Sockets bound to HIs, not to IP addresses
- HIs translated to IP addresses in the kernel



HIP as the new waist of TCP/IP



Protocol overview



Initiator

Responder

I1: HIT_I, HIT_R or NULL

R1: HIT_I, HIT_R, puzzle, DH^+_R, K^+_R, sig

I2: HIT_I, HIT_R, solution, DH^+_I, $\{K^+_I\}$, sig

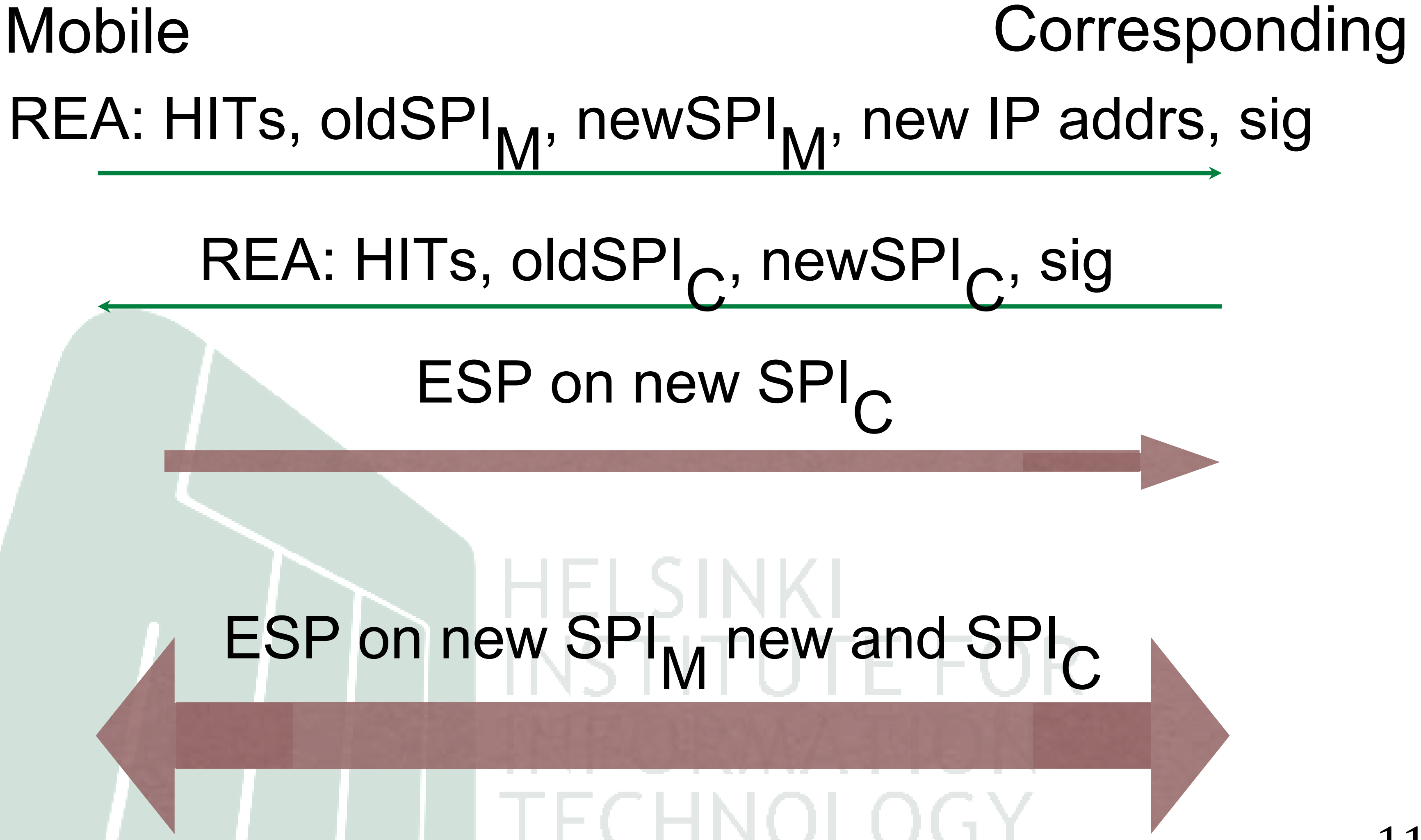
R2: HIT_I, HIT_R, sig

ESP protected messages

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

Mobility protocol



Mobile

Corresponding

REA: HITs, oldSPI$_M$, newSPI$_M$, new IP addrs, sig

REA: HITs, oldSPI$_C$, newSPI$_C$, sig

ESP on new SPI$_C$

ESP on new SPI$_M$ new and SPI$_C$

Rendezvous

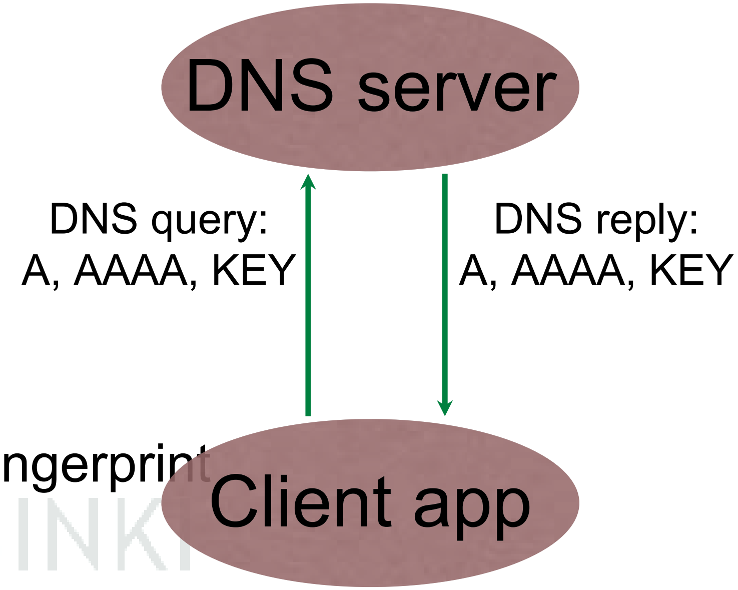
- Initial rendezvous
  - How to find a moving end-point?
  - Can be based on directories
  - Requires fast directory updates

→Bad match for DNS

- Tackling double-jump
  - What if both hosts move at same time?
  - Requires rendezvous point

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



Infrastructure research

- HIs currently 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
  - Need a data structure for flat data

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

HIP overlay and IPsec connectivity

- Overlay control plane between all hosts
  - DHT based flat routing overlay
  - Routes HIP control packets
- End-to-end IPsec between any two hosts
  - Firewalls opened dynamically
- Only end-to-end signalling (HIP)
  - User plane “reacts” to end-to-end signalling messages
- Host Identity Indirection Infrastructure (Hi3) combines i3 with HIP
  - Current prototype on PlanetLab (distributed testbed of 500 servers)

A Brief History of HIP

- Idea discussed briefly at 47th IETF in 1999
- Development “aside” the IETF since then
- IETF working group created in early 2004

- Base protocol more or less ready
  - Five known implementations (3 up-to-date and interoperating)
- WG re-charted this year, probably runs through 2007

IETF standardization status

Name	Cur version	Status
Ietf-hip-arch	-03	RFC4423
Ietf-hip-base	-06	IETF last call
Ietf-hip-esp	-03	IESG review
Ietf-hip-registration	-02	IESG review
Ietf-hip-dns	-08	IESG review
Ietf-hip-rvs	-05	IESG review
Ietf-hip-mm	-04	IESG review
Ietf-hip-api	-00	Mar 07?
ietf-hip-nat	-00	Mar 07?
draft-laganier-ipv6-khi	-05	IETF last call

Implementation status

- Five publicly known implementations
  - Ericsson Research Nomadiclab, FreeBSD/Linux
  - Helsinki University of Technology, Linux
  - Boeing Phantom Works, Linux/Windows/Mac OS
- Outdated
  - Andrew McGregor, Python user level
  - Sun Labs Grenoble, Solaris

Tekes *Infrastructure for HIP* Project

- Partners: HIIT, TKK, Nokia, Ericsson, Elisa, Finnish Defense Forces
  - 2,5 years, mid 2004-2006
- Project Goals
  - Study and develop the infrastructure support necessary for a wide deployment of HIP
  - Provide scientific results and play a role in the standardization of HIP
- InfraHIP II is coming too!

International Connections

- ICSI, Berkeley
  - Scott Shenker
- UC Berkeley
  - Ion Stoica, Anthony Joseph (at HIIT 8-11.2004)
- M.I.T
  - Hari Balakrishnan’s group
- RWTH, Aachen
- SICS, Sweden

InfraHIP Work Packages

1. *Next gen. Internet architecture*
2. *HIP on Linux*
3. *Rendezvous and naming*
4. *Multiple HIP identities*
5. *Application migration*
6. *HIP applications*
7. *Corporate HIP*

NordicHIP

- Andrei Gurtov, Martti Mäntylä, Bengt Ahlgren, Antti Ylä-Jääski
- Focus: Serve as a collaboration tool for national HIP activities by supporting mutual visits, summer schools, and some core technical work on Internet architecture, IPv4/v6 co-existence and naming infrastructure
- NORDUNET3 call
- Partners: HIIT/TKK, SICS, TML/TKK
- Duration: 2006-2009 (4 years)
- Project budget: 134 000 €/year

Potential HIP benefits for Grids

- IPv4-v6 interoperability
- Multihoming
- Denial-of-Service protection
- IPsec encryption of traffic
- Authentication
- NAT traversal
- Rendezvous support from Hi3
- Mobility/fault tolerance
- Wide-area application migration

NI HAO Grid

- EU project proposal for FP6 China call
  - Didn’t go through by one evaluation point…
- A practical project targeting EU-China Grid testbed with IPv6 and HIP
  - HIP can bridge IPv4 and IPv6 applications
- Implement HIP to Globus Toolkit GT3/OGSA (Java- and WebServices-based)

Thanks!

- More info on HIP at http://infrahip.hiit.fi, gurtov@hiit.fi
- Questions?