Infrastructure Support for Host Identity Protocol

Andrei Gurtov
Helsinki Institute for Information Technology

(HIP slides from Dr. Pekka Nikander, IAB member, Ericsson Research Finland)

Architectural background

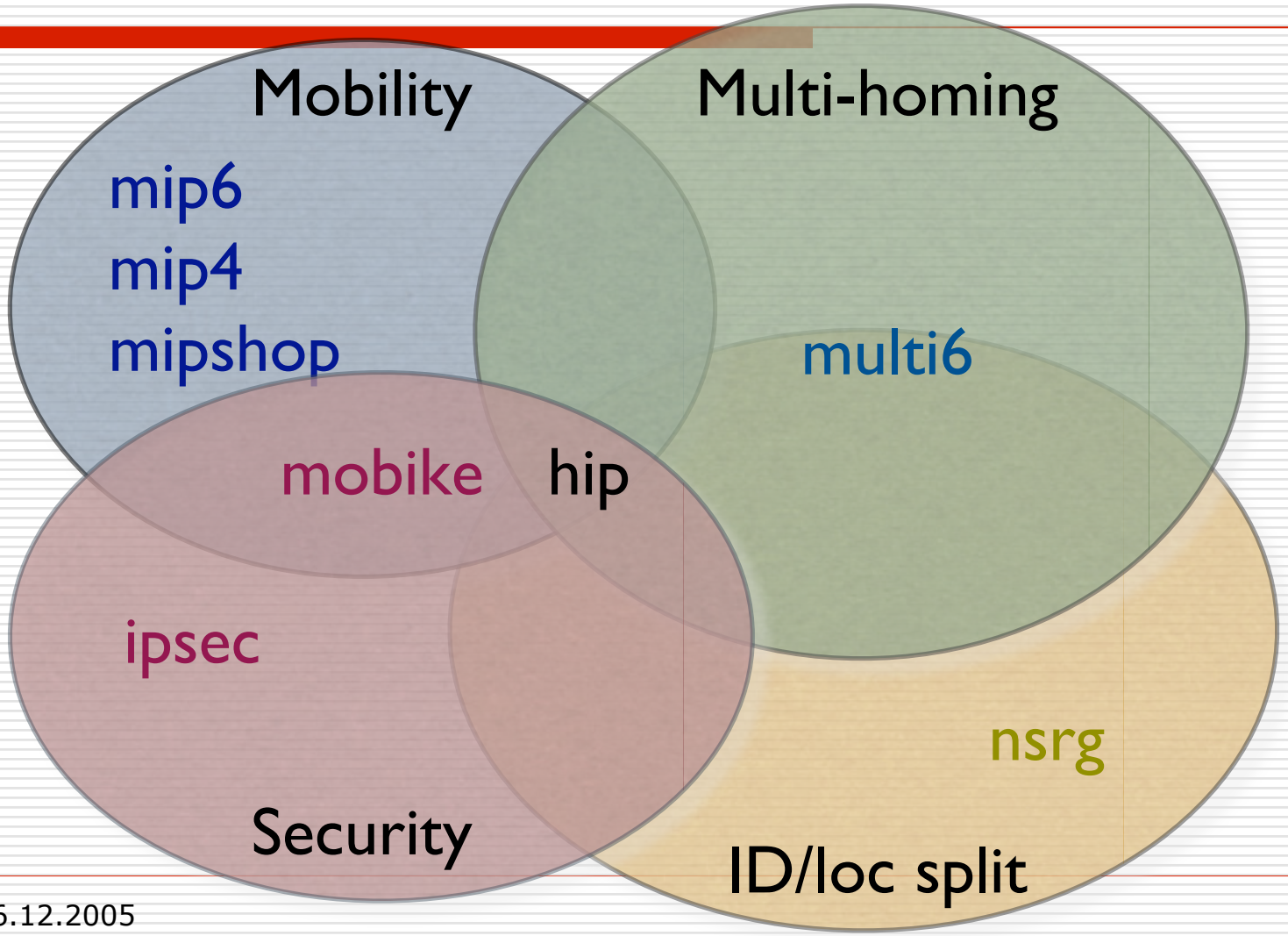
- IP addresses serve the dual role of being
  - End-point Identifiers
    - Names of network interfaces on hosts
  - Locators
    - Names of naming topological locations

- 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

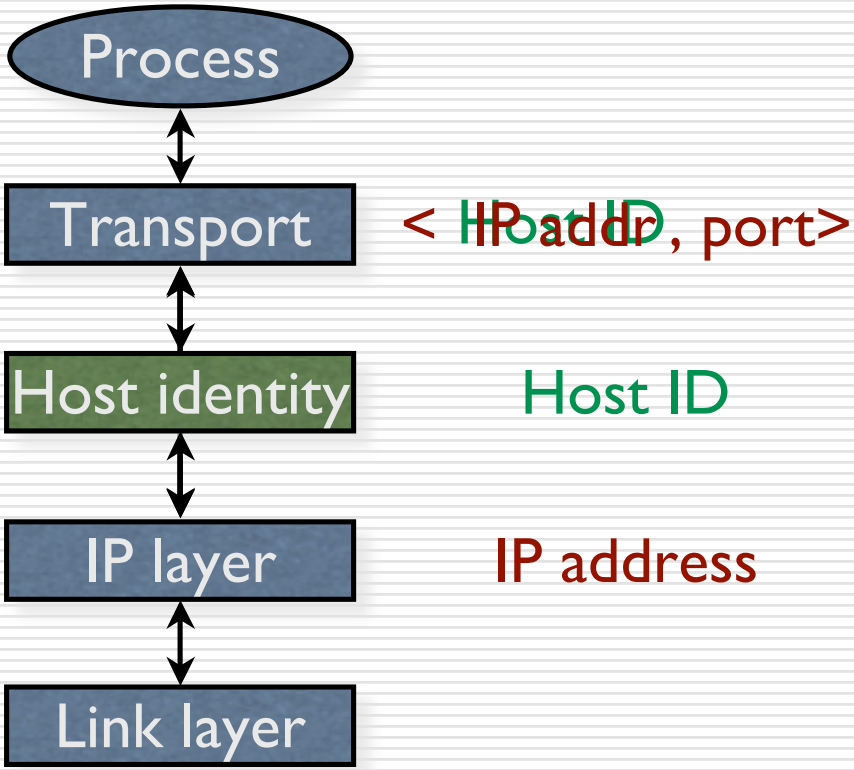


HIP in a Nutshell

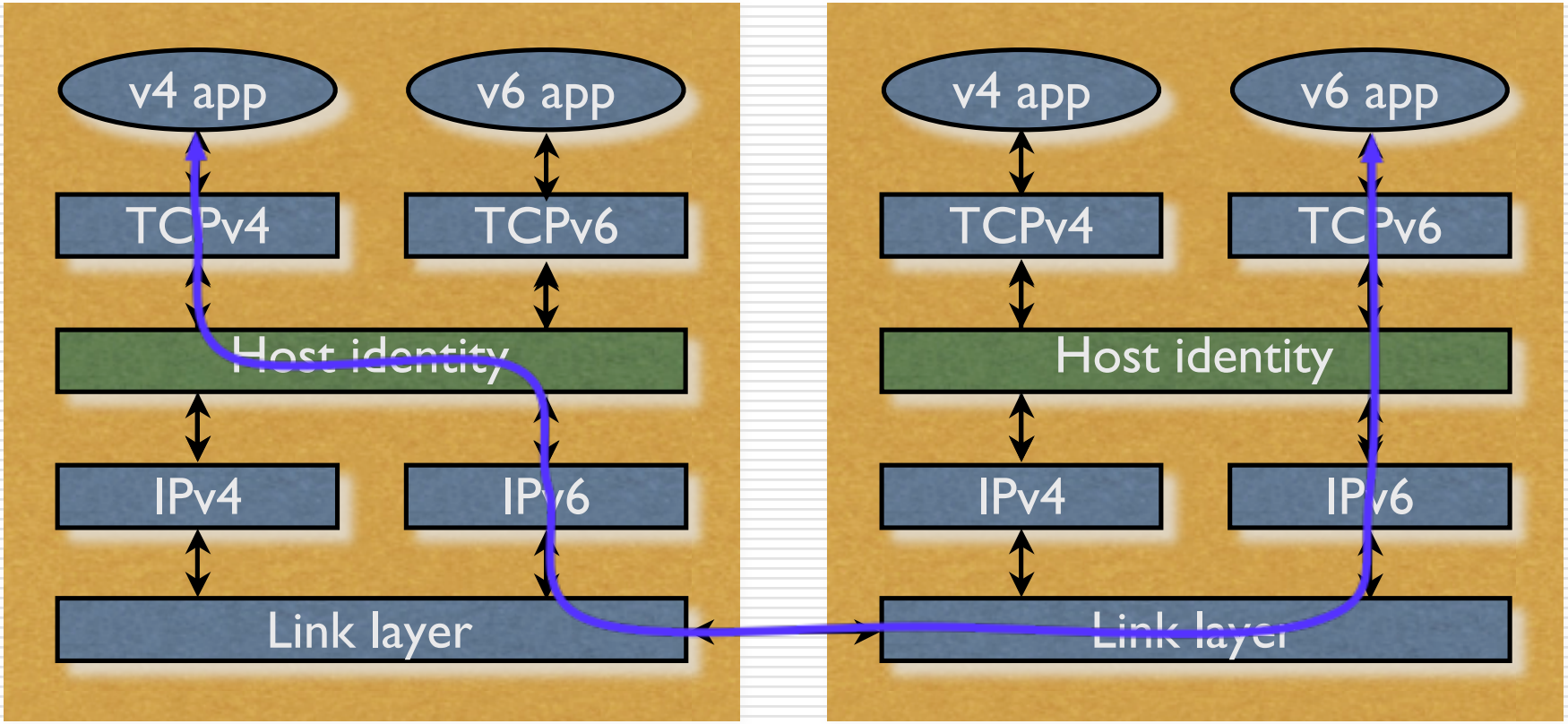
- Architectural change to TCP/IP structure
- Integrates security, mobility, and multi-homing
  - Opportunistic host-to-host IPsec ESP
  - End-host mobility, across IPv4 and IPv6
  - End-host multi-address multi-homing, IPv4/v6
  - IPv4 / v6 interoperability for apps
- A new layer between IP and transport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

The Idea

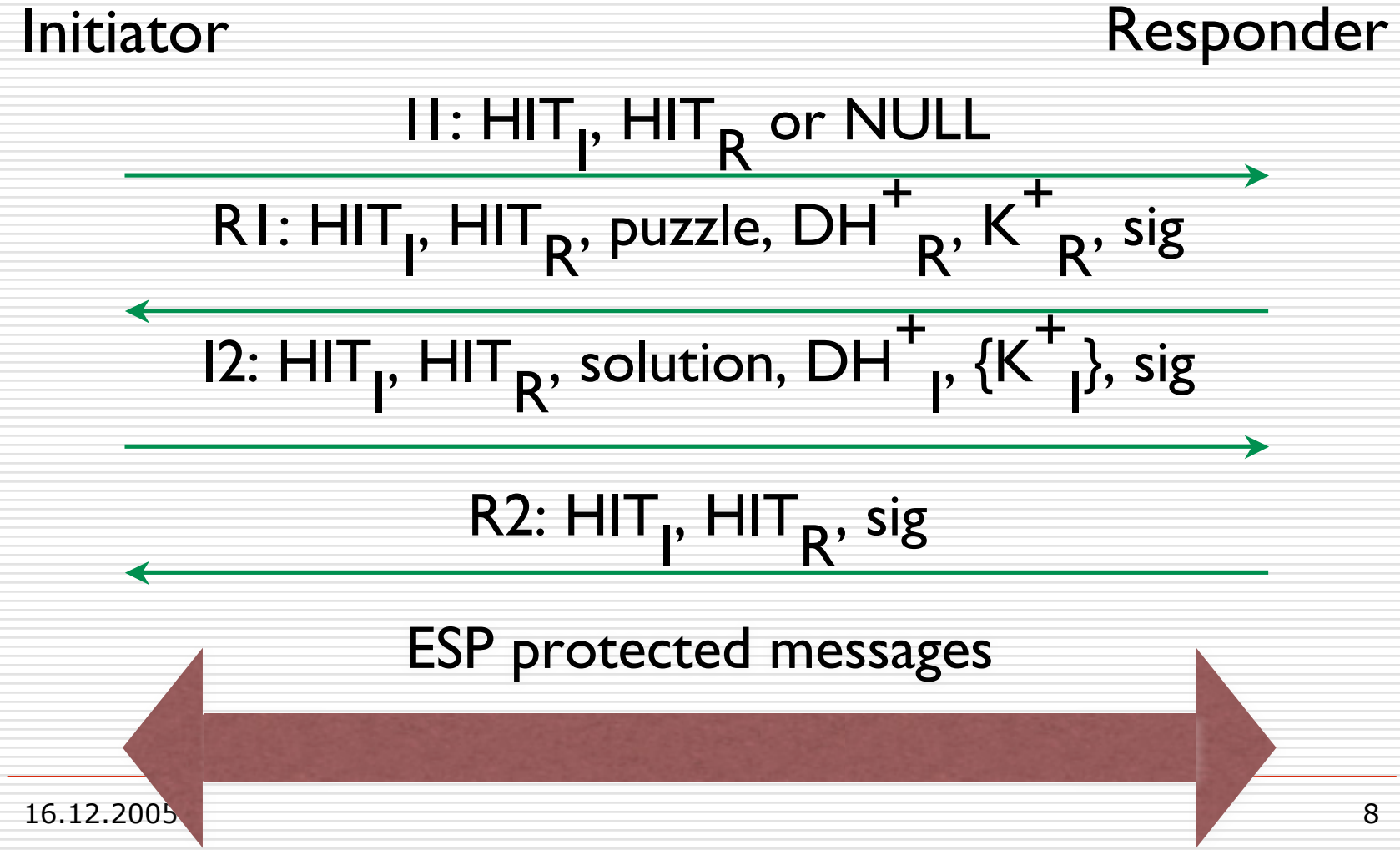
- A new Name Space of Host Identifiers (HI)
  - Public crypto keys!
  - Presented as 128-bit long hash values,
    Host ID Tags (HIT)
- Sockets bound to HIs, not to IP addresses
- HIs translated to IP addresses in the kernel



HIP as the new waist of TCP/IP



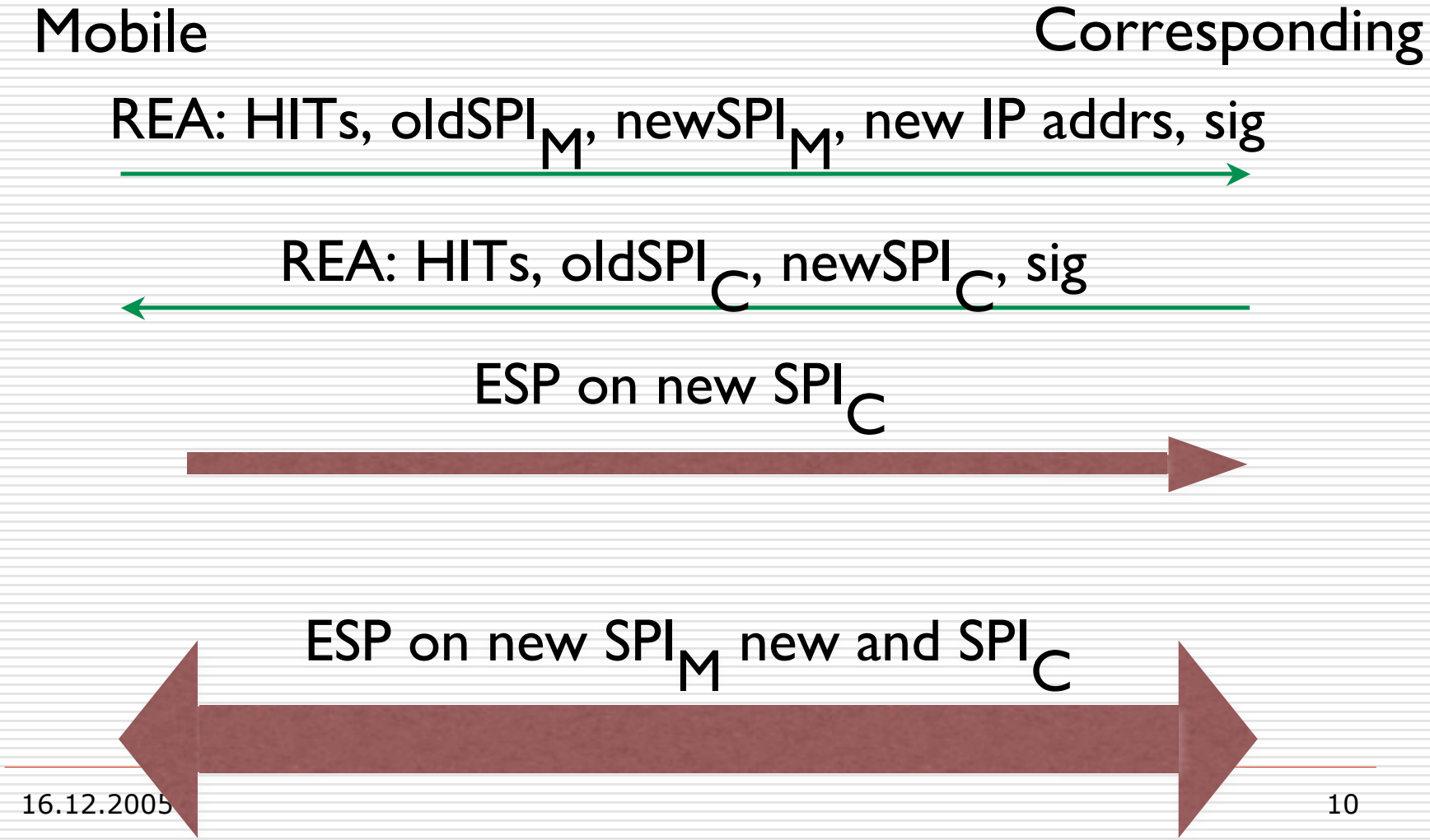
Protocol overview



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



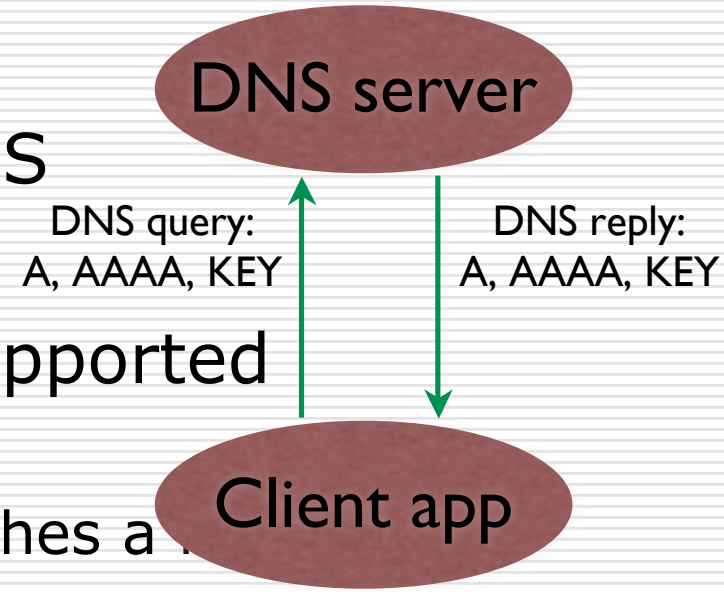
Rendezvous

- 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



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

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, interoperating implementations
- More work needed on mobility, multi-homing,
NAT traversal, infrastructure and other issues

IETF standardization status

Draft	Curr. vers.	at IESG
ietf-hip-arch	-03	now
ietf-hip-base	-pre-02	fall 2005?
ietf-hip-esp	-pre-00	fall 2005?
ietf-hip-registration	-pre-00	fall 2005?
ietf-hip-dns	-01?	fall 2005?
ietf-hip-rvs	-00	early 2006?
ietf-hip-mobility	-mm-02	early 2006?
ietf-hip-multihoming	-mm-02	late 2006?

Implementation status

- Five publicly known implementations
  - Ericsson Research Nomadiclab, FreeBSD
  - Helsinki University of Technology,
  - Boeing Phantom Works, Linux
  - 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 2004-2007
- Project Goals
  - Study and develop the infrastructure support necessary for a wide deployment of HIP.
  - Provide scientific results and play a leading role in the standardization of HIP

People Involved

- Doc. Pekka Nikander, Prof. Martti Mäntylä (HIIT)
- Prof. Antti Ylä-Jäaski (TKK)

- Andrei Gurtov, PhD, project manager
- Teemu Koponen, MSc
- Miika Komu, MSc
- Mika Kousa, ~MSc
- Dmitry Korzun, PhD
- Abhinav Pathak
- Janne Lindqvist, MSc
- Essi Vehmersalo
- Niklas Karlsson

International Connections

- ICSI, Berkeley
  - Scott Shenker
- UC Berkeley
  - Ion Stoica, Anthony Joseph (at HIIT 8-11.2004)
- M.I.T
  - Hari Balakrishnan
- Meetings so far
  - Collaboration meeting, Berkeley, 11/04
  - HIP Workshop, Washington, 11/04
  - OASIS retreat and i3 meeting, Tahoe, 1/05
  - OASIS retreat 6/5
  - Two people at ICSI for summer 2005

InfraHIP Work Packages

- ***Next gen. Internet architecture***
- ***HIP on Linux***
- ***Rendezvous and naming***
- ***Multiple HIP identities***
- ***Application migration***
- ***HIP applications***
- ***Corporate HIP***

WP1. Architectural

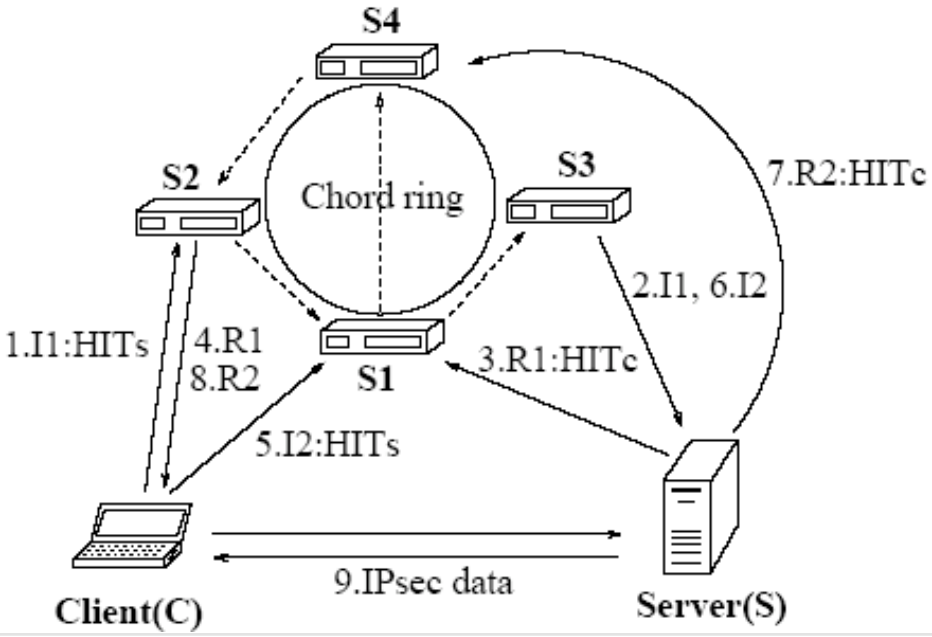
- Explore the general effect of identifier/locator split on Internet
- Study alternative solutions to HIP
  - Internet Indirection Infrastructure
  - Multi6, Mobile IP, …
- Produce a report on findings
  - Comparison criteria for existing alternatives to HIP
- Cooperate on integrating HIP as one component of the next-generation Internet architecture

WP2. HIP on Linux

- Finalize HIIT's HIP implementation in Linux kernel
- Release as open source, maintained, and easily usable software
- Integrate into official Linux kernel
- Performance evaluation of HIP exchange and mobility
- Regular interop testing with other implementations at IETF
- Demonstrations
- Further development of native HIP API
- Mobility extensions with multiple Security Associations (SAs)

WP3. Rendezvous & Naming

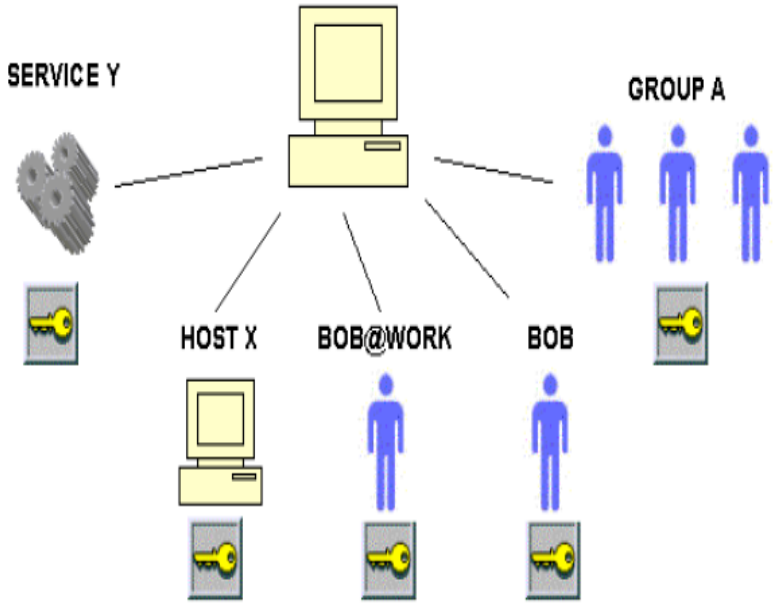
- Infrastructure for resolving Host Identities to IP addresses
  - DNS Extensions
  - Use of Distributed Hash Tables or i3 systems
  - Rendezvous servers
- Deploy an experimental infrastructure on a wide-scale testbed PlanetLab



WP4. Multiple Identities

- How to manage and store multiple host identifiers on a single operating system
  - Needed e.g. for privacy protection
- Major extensions to HIP API and implementation

Various entities with HIP identities inside a host.



WP5. Application Migration

- Study migration of a running HIP application between hosts
  - Maintaining communication transparency
  - Avoiding residual dependency
- Delegation-based approach
  - Destination re-establishes the associations with remote peers
  - Destination receives an authorization to use old HIT using a signed certificate
- Implementing a prototype using ZAP migration system from Columbia University

WP6. Applications for HIP

- Evaluate new possible applications enabled by HIP
- ”Road warrior” = mobile VPN user
  - E.g. distributed file system with back-up
- Search in peer-to-peer systems
- Faster WLAN access control
- Device peering
- Ad-hoc networking

WP7. Corporate

- Study use of HIP in the corporate sector
- NAT/Firewall traversal
- Group communication
- Management of HIP hosts, MIBs
  - Make network renumbering easier
- VPN solutions

Summary

- New cryptographic name space
  - IP hosts identified with public keys
- Integrates security, mobility, multi-homing
- Initial ideas at the IETF in late 1999
- Base specifications start to be mature
- Five interoperating implementations
  - http://infrahip.hiit.fi
  - http://www.hip4inter.net
  - http://www.tml.hut.fi/~pnr/publications/
- InfraHIP develops extensions to naming and middleboxes necessary for widespread deployment of HIP