Infrastructure Support for Host Identity Protocol

COST 290 meeting, Colmar

Andrei Gurtov
Helsinki Institute for Information Technology

(HIP slides from Pekka Nikander, Ericsson Research Finland)

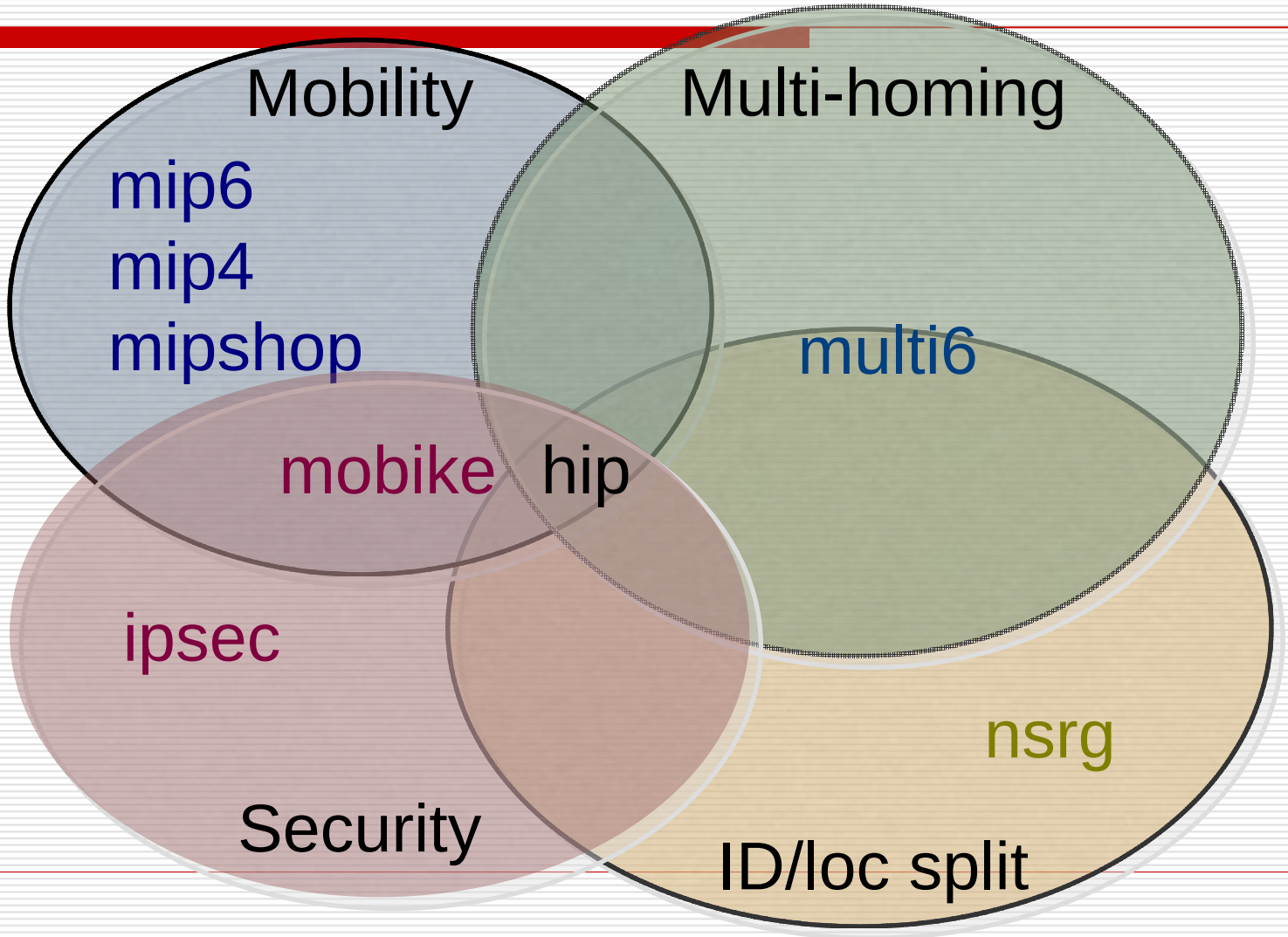
Architectural background

- 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

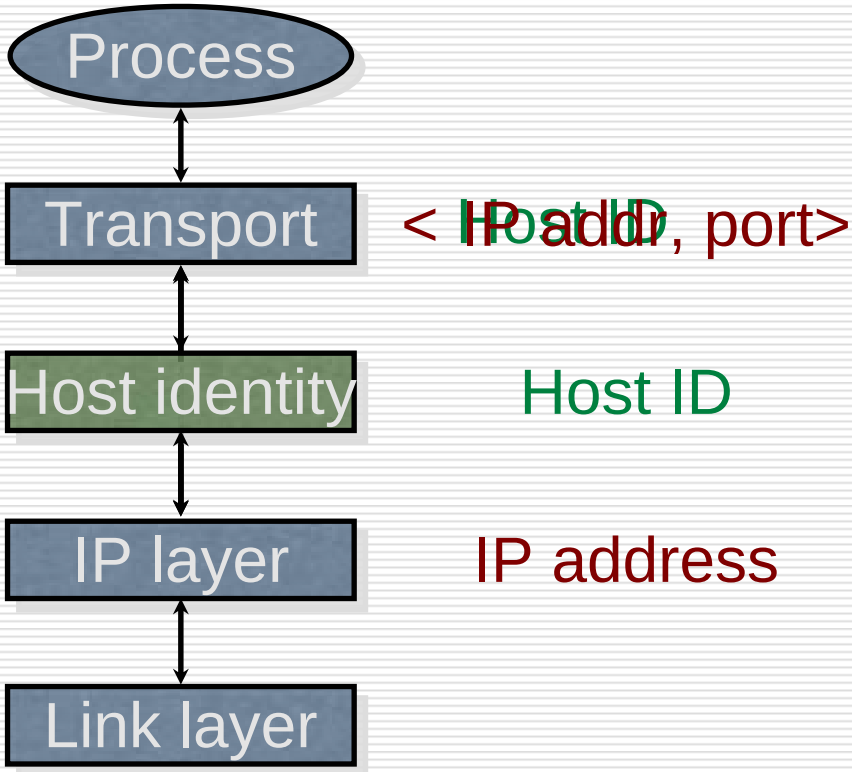


HIP in a Nutshell

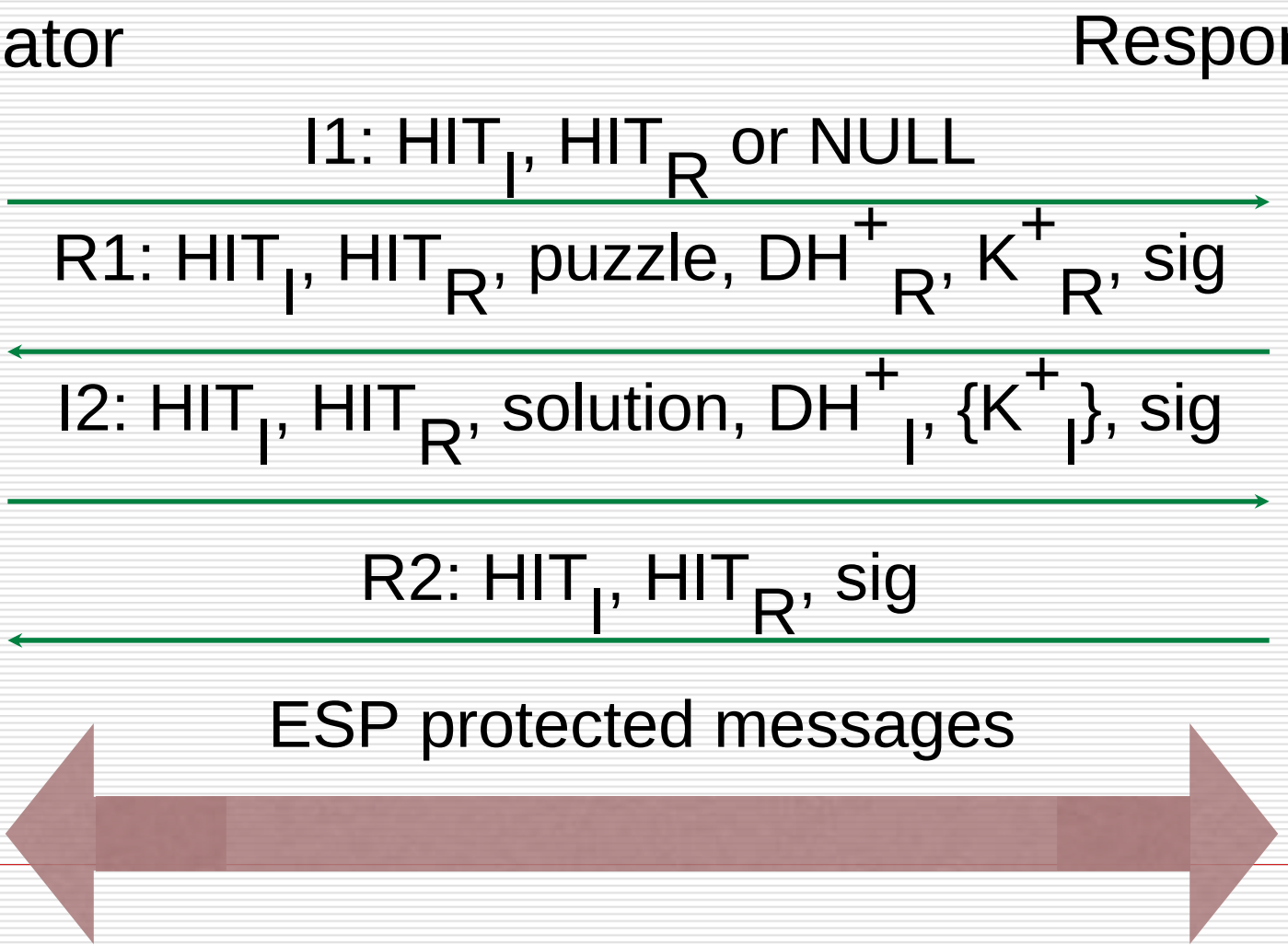
- Architectural change to TCP/IP structure
- Integrates security, mobility, and multi-homing
  - Opportunistic host-to-host IPsec ESP
  - End-host mobility, across IPv4 and IPv6
  - End-host multi-address multi-homing, IPv4/v6
  - IPv4 / v6 interoperability for apps
- A new layer between IP and transport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



Protocol overview



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?

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-Jääski (TKK)

- Andrei Gurtov, PhD, project manager
- Teemu Koponen, MSc
- Miika Komu, MSc
- Mika Kousa, ~MSc
- Dmitry Korzun, PhD
- Wenpeng Zhou, MSc
- 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

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***

WP1. Architectural

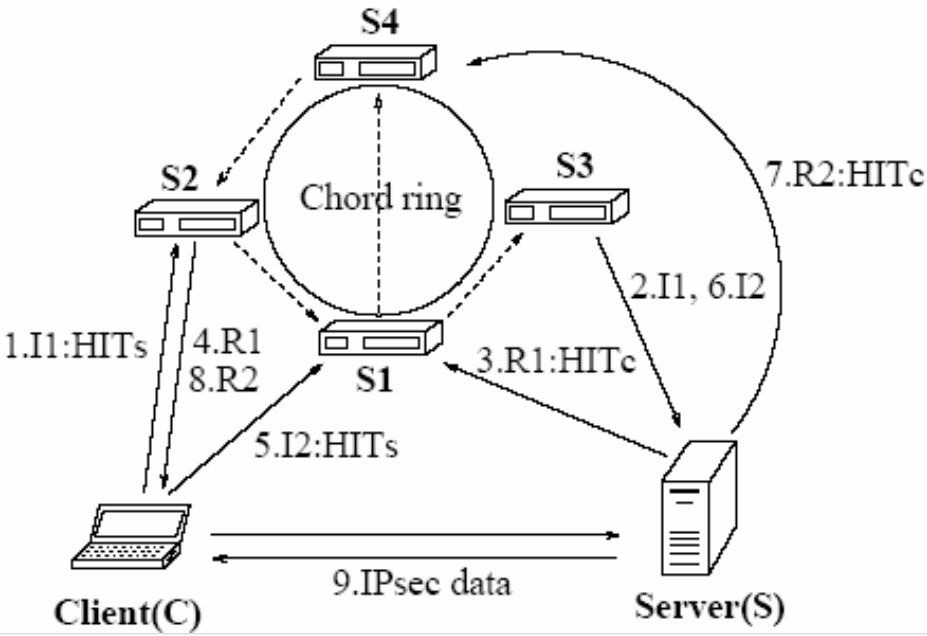
- Explore the general effect of identifier/locator split on Internet
- Study alternative solutions to HIP
  - Internet Indirection Infrastructure
  - Multi6, Mobile IP, …
- Produce a report on findings
  - Comparison criteria for existing alternatives to HIP
- Cooperate on integrating HIP as one component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

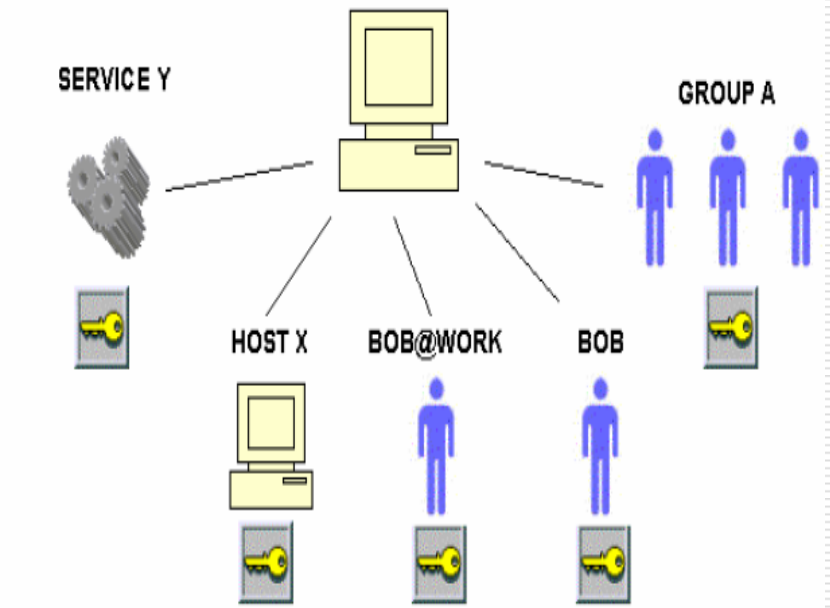
- Infrastructure for resolving Host Identities to IP addresses
  - DNS Extensions
  - Use of Distributed Hash Tables or i3 systems
  - Rendezvous servers
- Deploy an experimental infrastructure on a wide-scale testbed PlanetLab



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://hipl.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