SPEAR: A secure P2P communication platform on mobile Linux

Joakim Koskela, Andrei Gurtov

HIIT and CWC Oulu

5.10.2011

Mobile Linux Summit

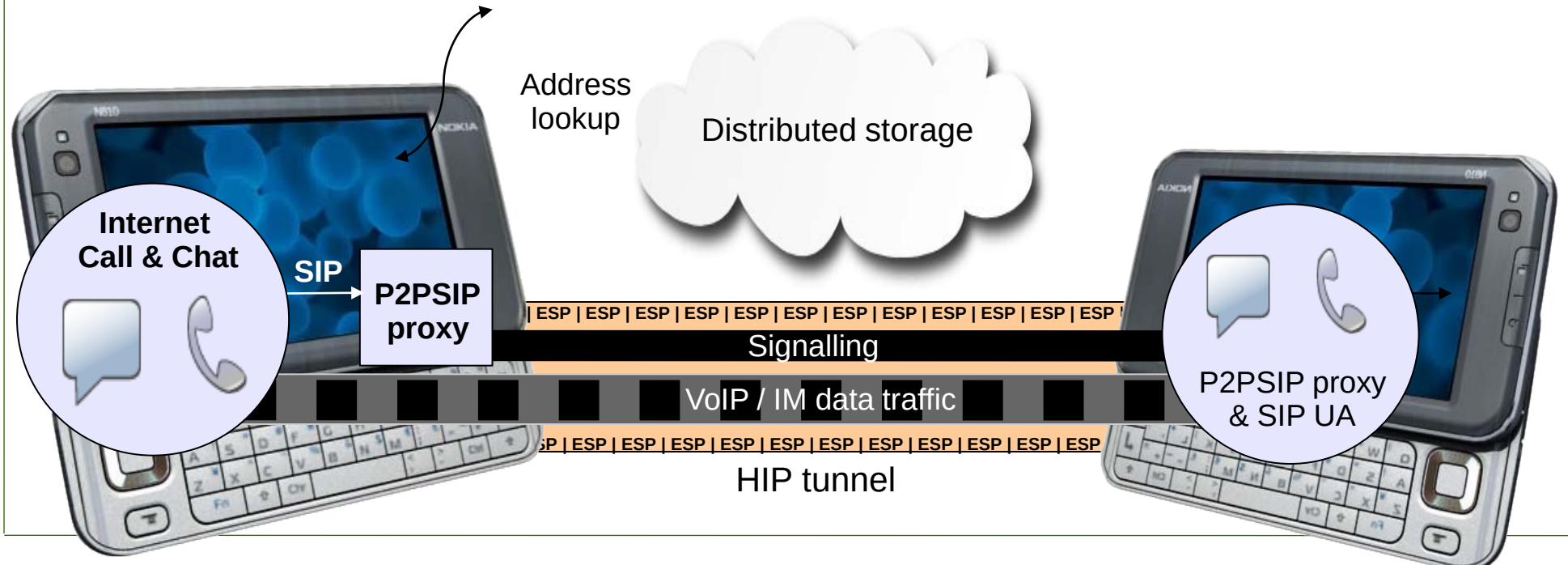
HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

SPEAR

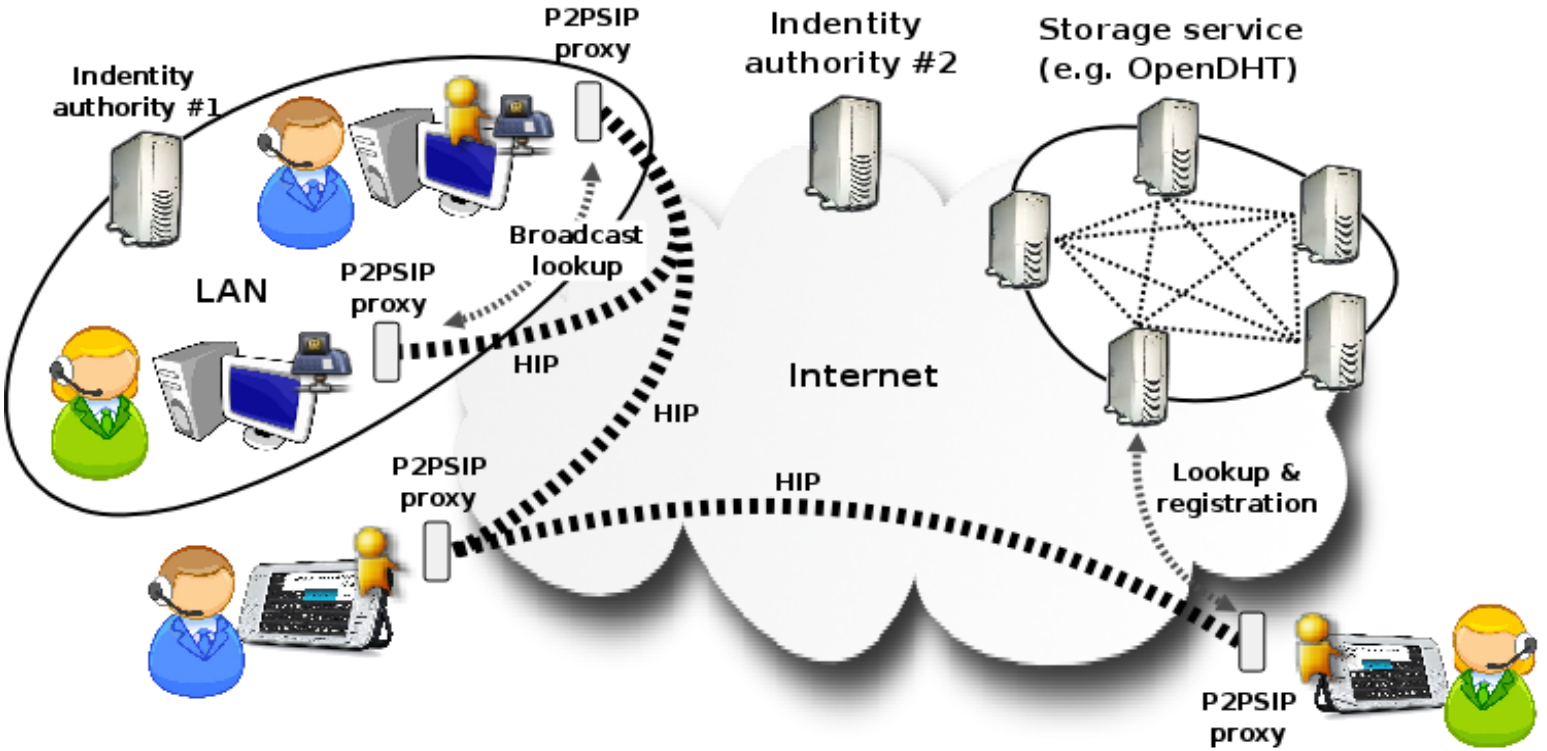
- A tool for studying security and novel features in P2P
  - Trust & reputation-based SPAM prevention in P2P networks
  - Confidentiality, privacy, secure architectures
  - Distributed voicemail, multi-party conferencing
- Implemented on Linux/Maemo (N810 main target device)
- Host Identity Protocol used for all peer-to-peer connections
- VoIP operator servers replaced by one of more *distributed storages*
  - Currently OpenDHT, HTTP storage & LAN multicast supported
- Privacy extensions
  - Prevent overlay nodes from recording our call log
- Social trust-path based SPAM prevention
  - “Accept calls only from friends-of-friends”

Prototype architecture

- Implemented as a local SIP proxy for legacy SIP user agents (UAs)
  - The N810 Internet Call application is used as front-end
- The proxy provides the same services as a traditional client-server SIP proxy, but using a distributed back-end
  - No central repository or reliance on DNS
- The distributed storage is used for lookup of peer HIT and locators
  - HIP used for further communication



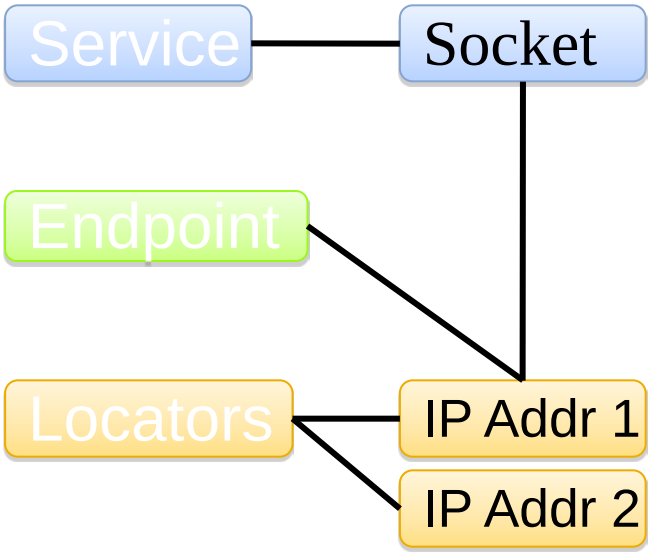
System overview



- Identities are bound to HITs using certificates
  - Issued by trusted identity authorities
- Multiple identity authorities supported
  - Anyone can create an authority for a specific purpose

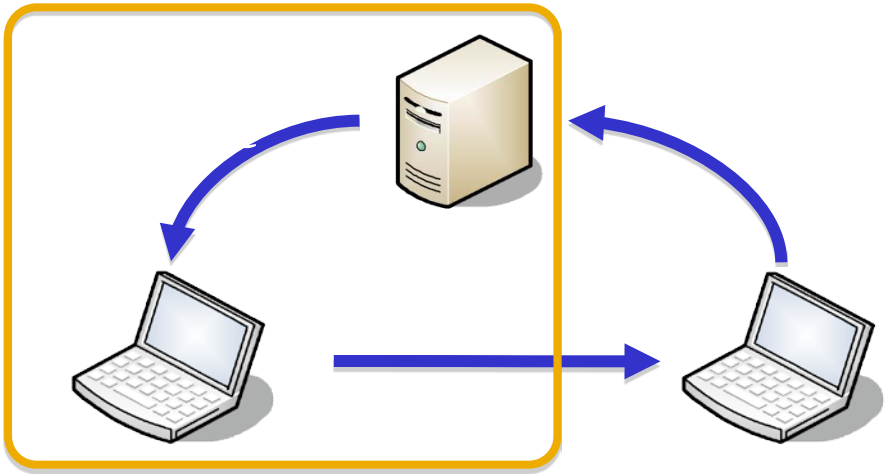
Today's Internet Infrastructure and Protocols

- Current Internet uses the TCP/IP stack
  - Developed for non-mobile, single-homed hosts
    - Dual role of IP addresses: identify and locate end-hosts
  - Offers no security mechanisms
    - End-hosts cannot prove their identities
    - No data confidentiality and integrity protection
- Additional protocols extend specific IP functionality
  - Mobility support: Mobile IP, …
    - Requires additional infrastructure elements (*see next slide*)
  - Security: IPsec, ...
    - Requires session setup → e.g. with IKE protocol

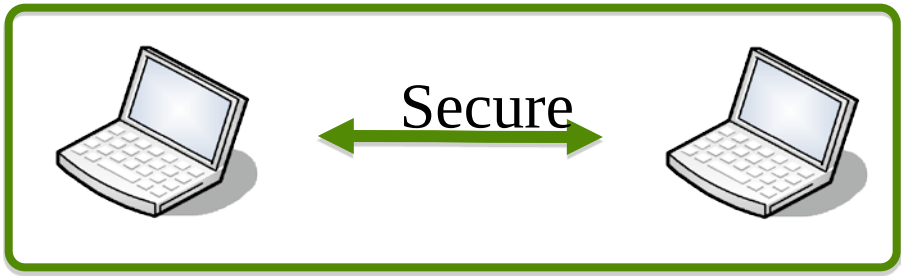


HIP vs. Mobile IP in a Nutshell

- Mobile IP
  - Home agent as fixed point
  - Support for un-modified correspondent node
  - Indirect mobility management
  - Triangular routing
  - Infrastructure support (FA, HA)
- Host Identity Protocol
  - End-to-end associations
  - HIP-aware end-hosts
  - Direct mobility management
  - Authentication
  - End-to-end security
  - No infrastructure support needed (in most cases)

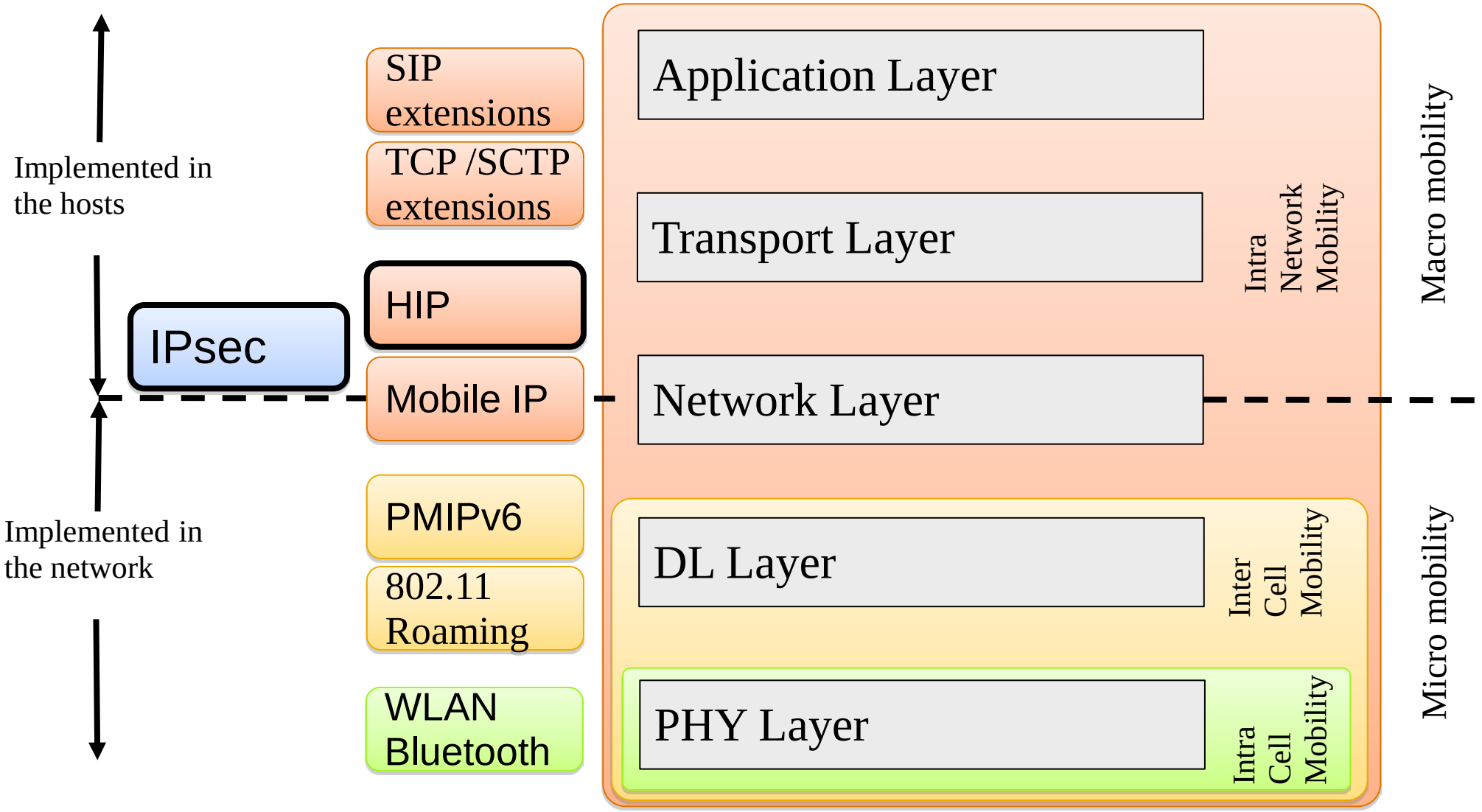


Mobile IP No Mobile IP

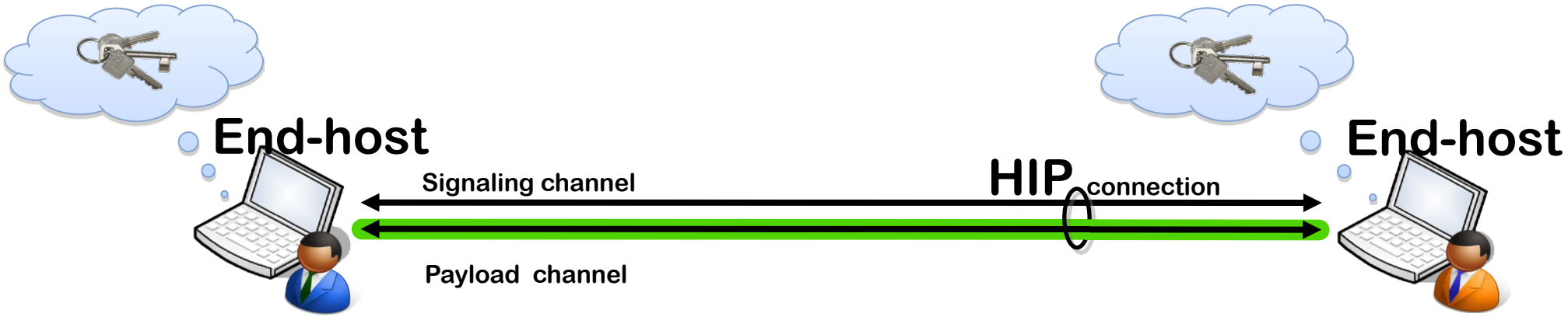


HIP

Mobility in the Network Stack



Host Identity Protocol (HIP)



Signaling and key-exchange protocol

- Separate control and payload channel
- Allows use of security services → e.g. IPsec payload channel
- Similar to Internet Key Exchange (IKE)

Introduces new namespace

- Namespace is cryptographic in nature
- Provides support for mobility and multi homing

HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Cryptographic Namespace

Host authentication is essential when supporting mobility and multi homing

- End-hosts have to verify they still talk to the same peer
- State changes at middleboxes may be required

Self-generated public and private key-pair provides the host identity (HI) in HIP

- RSA by default, DSA also supported in HIP specification
- Length of the public key - 512, 1024 or 2048 bits
- Abstraction required for use in network stack due to large and variable size of the public key
- →Two additional forms of host identities: HIT and LSI

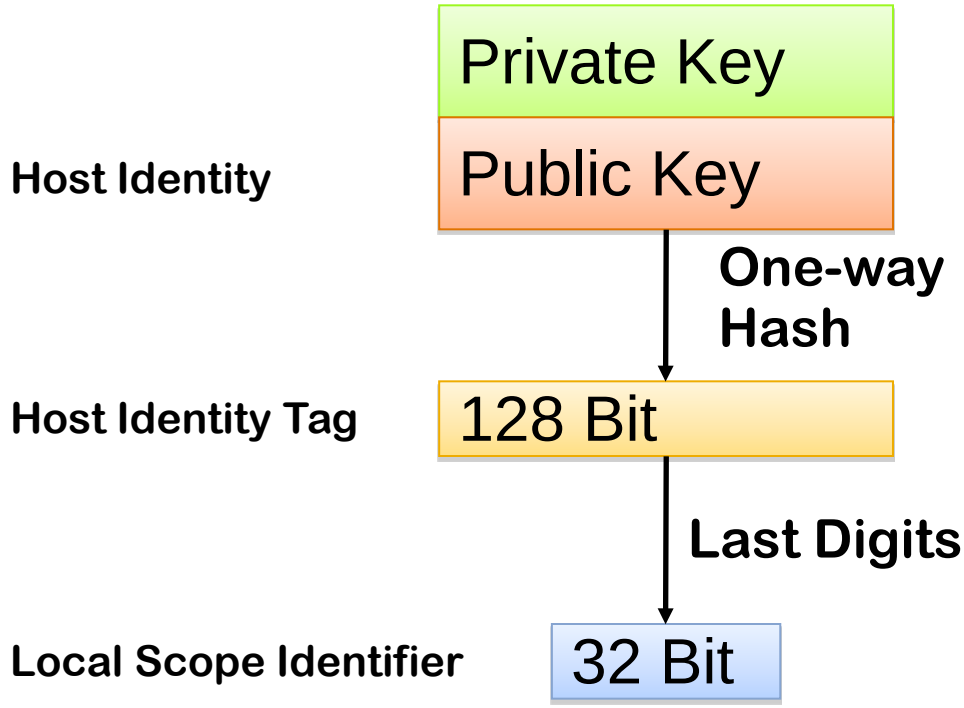
Globally Unique and Locally Unique Identifiers

Host Identity Tag (HIT)

- Compatible with IPv6 address
- Statistically unique
- Probability of collisions is negligible

Local Scope Identity (LSI)

- Compatible with IPv4 address
- Probability of collisions is significant
- →Restricted to local scope



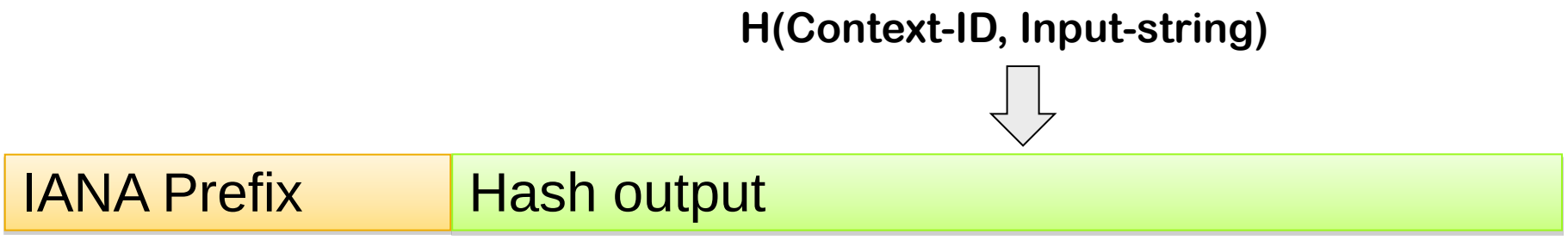
HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Computation of a HIT

HIT generation follows the Overlay Routable Cryptographic Hash ID (ORCHID) method

Components of a HIT

- Not routable IPv6 prefix assigned by IANA (2001:0010::/28)
- 100-bit string extracted from SHA1 hash over 128-bit context ID and input string
  - Context ID – randomly chosen value for HIP
  - Input string must be statistically unique (here: public key)



HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Identifier / Locator split

Major problem in the original Internet architecture:

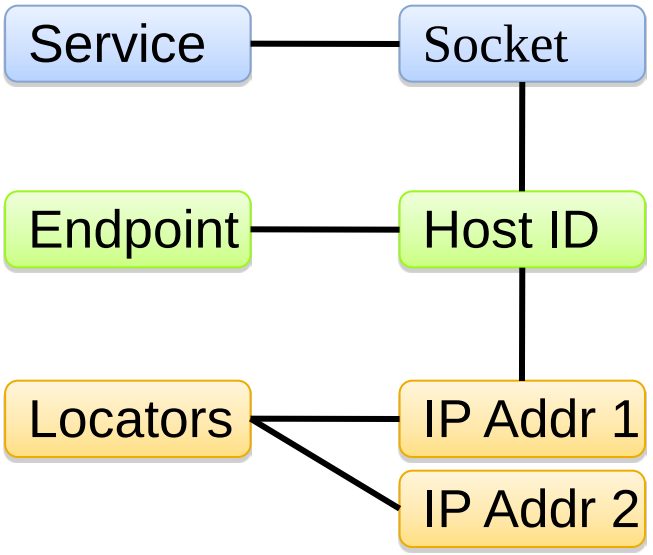
- Tight coupling between networking and transport layers (e.g. TCP checksum calculation)
- Mobility breaks transport layer connections

Separation of location and identity of networked hosts

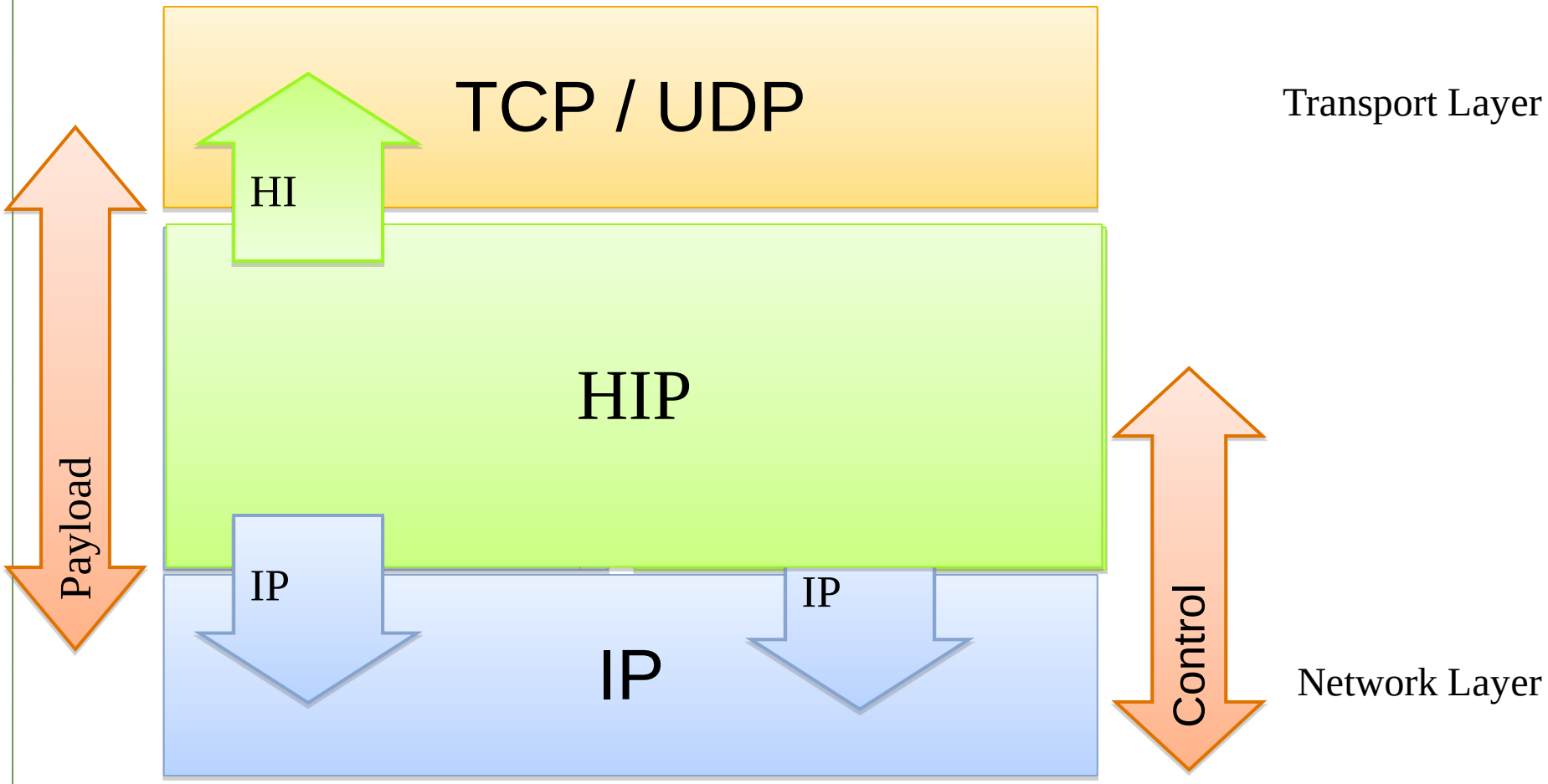
- HIP replaces role of IP as identifier
- IPv4 and IPv6 run underneath HIP
- Transport protocols bind to His

Benefit

- Applications see stable identity instead of a locator
- Routing decisions still based on locator
  - No changes to core infrastructure required



HIP in the Communication Stack



HIP Mobility in a Nutshell

137.11... | 1187:A...

Mapping:
1121:B... = 128.12...

I'm 1121:B...
Here is my
IPsec info

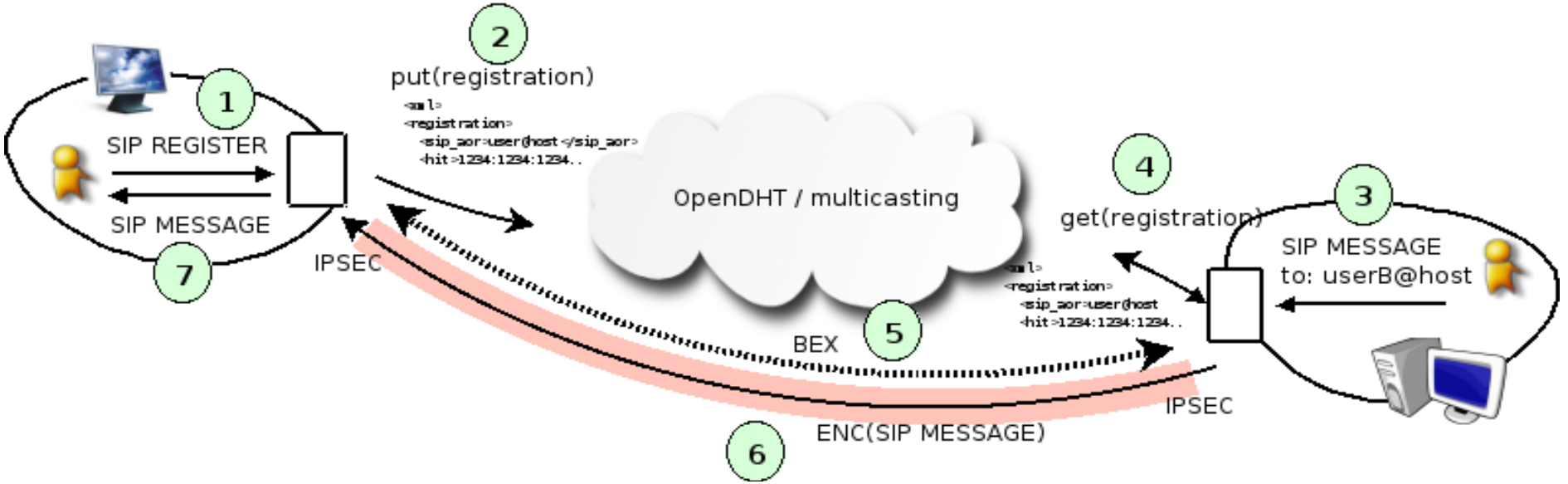
1121:B...

I'm 1187:A...
My IP:
137.22...

Mapping:
1187:A... = 80.210...

137.22... | 1187:A...

Signalling example



- SIP signaling is interpreted
  - REGISTER resulting in publishing locator information
  - SUBSCRIBEs kept track of for constructing buddy-relationships
- When a message destined for a peer is received, the proxy performs a lookup and establishes a HIP connection

HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Distributed voice mail 1/2

- Leave recorded messages for a recipient
  - When recipient is busy or offline
- Invite-advertise-acknowledge- scheme
  - Potential recipients leave *invites* for voice mail in the overlay
    - Either public or just for the users he is willing to receive voice mail from
    - Contains *greetings*, supported codecs, size limitations, storage info
      - Greetings are pre-recorded audio messages (“Please leave a message after the beep..”)
  - After recording a voice mail, an *advertisement* is left in the overlay
    - Using instructions found in the invite
  - After retrieving the voice mail, (optional) *acknowledgement*
    - Signals data maintainers that the voice mail can be deleted
- *Greetings* and *voice mails* are stored using different resources
  - Peers, the overlay, web-sites, cloud-based storage etc
  - Flexible URL scheme (http://, p2p://, dropbox:// etc)

Internet call application

SPEAR

Overlay and storage

Call alice

Where is alice?

Voice mail invite?

Invite for alice

Fetch greeting.mp3

Alice not found

Answer

Simulate Alice answering the phone

Play greeting.mp3

Record voicemail.mp3

Store voicemail.mp3

Store advertisement

SPEAR

Internet call application

REGISTER

Publish invite

Alice offline

Fetch voice mail advertisements

REGISTER

Fetch voicemail.mp3

Voicemail: ONLINE

Call voicemail

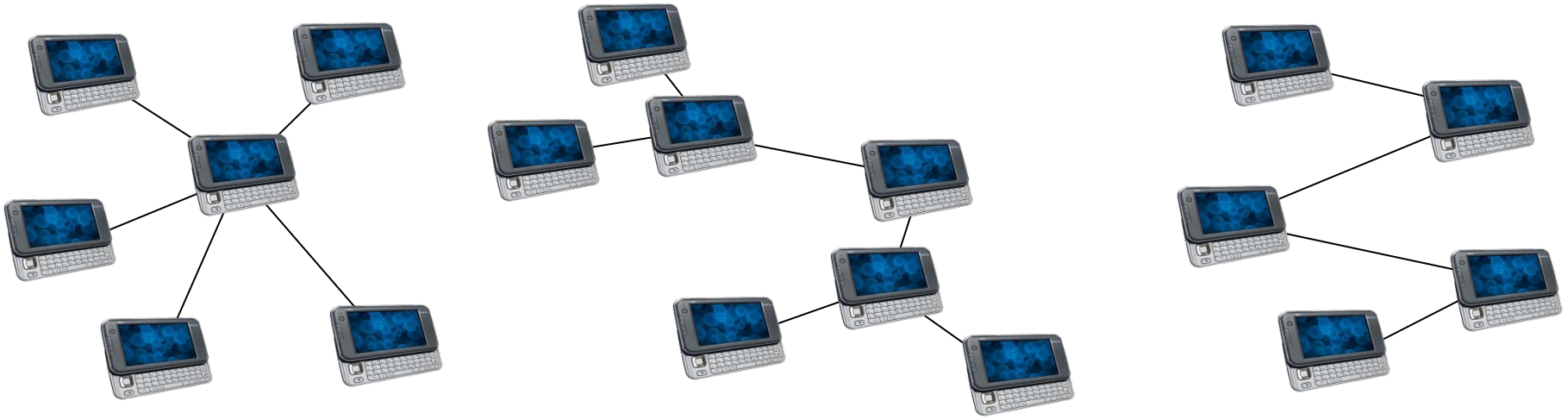
Play back message

Play voicemail.mp3

HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Multiparty conferencing 1/2

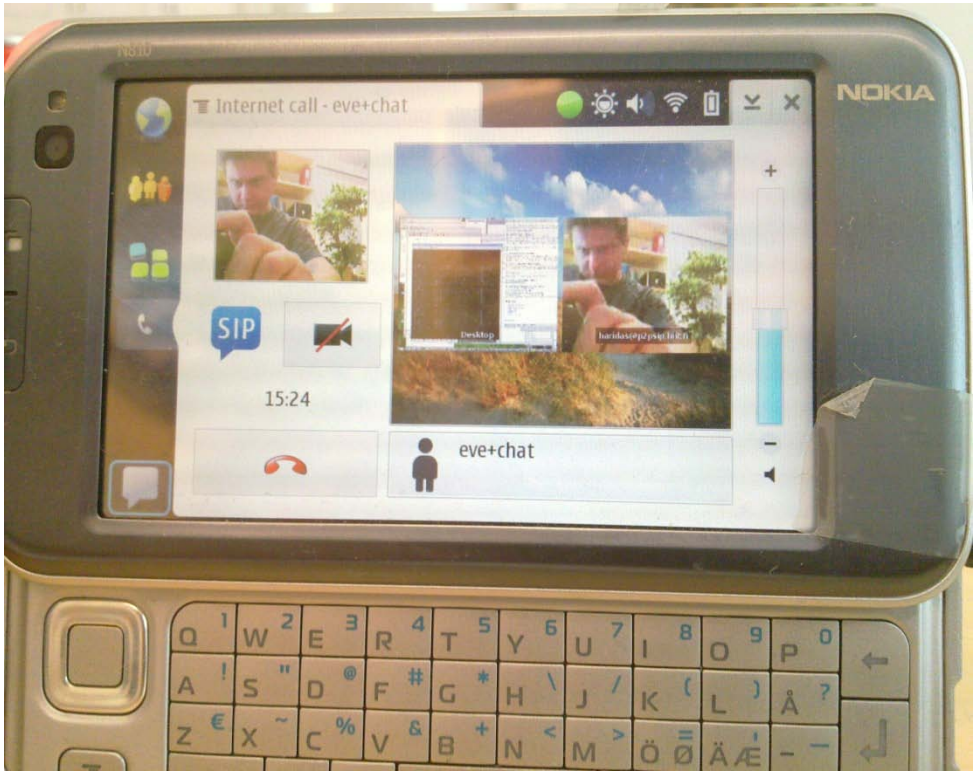
- Each SPEAR peer can act as a multiparty conference mixer
  - As SPEAR controls the signaling, media streams are intercepted too
  - Audio, video and instant messaging
  - Works with all SIP clients
- Multiparty *groups* are formed using an identity extensions
  - E.g., **`sip:alice+multiparty@hiit.fi`**
  - Future: public-key based group identities
- Different connection topologies possible
  - Centralized, distributed, hybrid



HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Multiparty conferencing 2/2

- Several extensions (plug-ins) implemented:
  - Audiorecording, screen casting, video / audio playback
  - Different backgrounds & layouts for video conferencing



HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Thanks for attention!

Next step: Integration with 3D Virtual World (RealXtend)

More info: http://p2psip.info/

Open source code: http://code.google.com/p/p2pship/

Authors: http://www.ee.oulu.fi/~agourtov/

See also:

J. Koskela, K. Karvonen, T. Kilinkaridis, A. Gurtov, Secure and usable P2P VoIP for mobile devices, In Proc. of the 12th ACM international conference on Human computer interaction with mobile devices and services (MobileHCI), September 2010

J. Koskela, A. Gurtov, A Secure Peer-to-Peer Web Framework, in Proc. of IEEE International Workshop on Data Security and PrivAcy in wireless Networks (D-SPAN 2010), June 2010.