HIP Location Privacy Framework

Alfredo Matos, Justino Santos, Susana Sargento and Rui Aguiar
{alfredo.matos,jsantos}@av.it.pt , {ssargento,ruilaa}@det.ua.pt
Institute of Telecommunications, Univ. Aveiro

João Girão and Marco Liebsch
{joao.girao,marco.liebsch}@netlab.nec.de
NEC Europe

Overview

- Motivation
- Host Identity Protocol
- Location Privacy Architecture
- IPv6 Instantiation
- Conclusions

Motivation

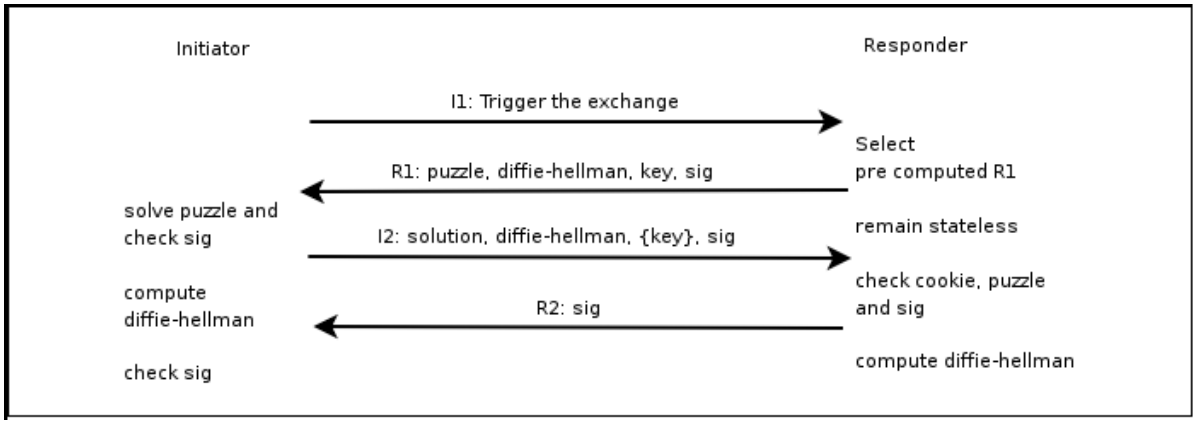
- Location privacy is a growing requirement
  - Users don't wish to be tracked
- Current Internet architecture does not provide location privacy
  - A topological location can give an accurate geographical position
- Why Host Identity Protocol (HIP) as base for a location privacy framework?
  - HIP decouples identifier and locator
  - Separate layers provide more "space" for a location privacy solution

Host Identity Protocol (HIP)

- 3.5 Protocol
  - Shim between Network and Transport Layers
- New cryptographic Namespace
  - Public/Private Key pairs
- Uses Host Identity Tags
  - Hash of 128 bits (same size as an IPV6)
  - No changes required in the applications
- Supports Mobility
  - Locator agility

Host Identity Protocol (II)

- Base Exchange (BE)
  - Cryptographic four-way handshake
  - Exchanges Identities (Public Keys)
  - Establishes bidirectional Security Associations
  - Bound end to end tunnels

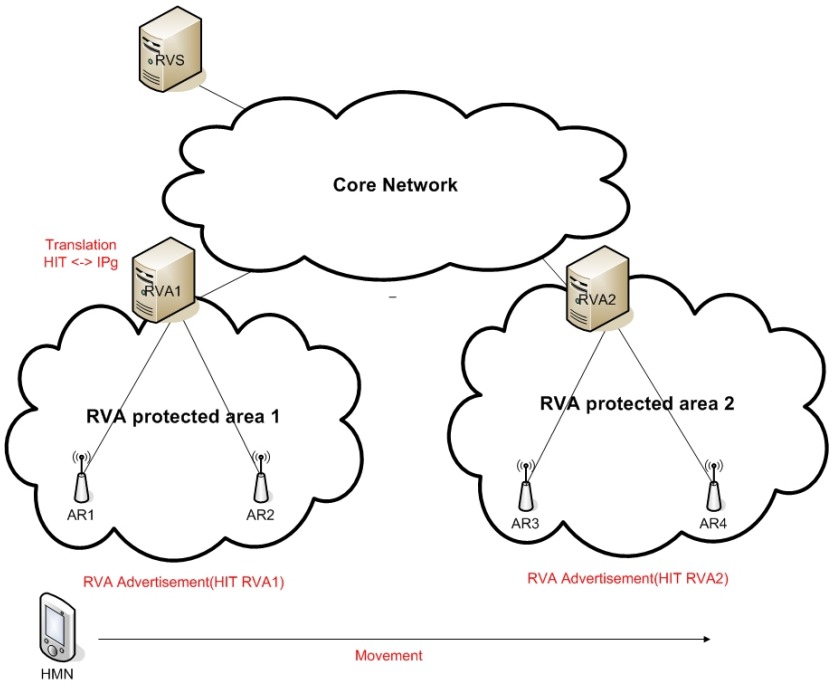


Location Privacy

"... location privacy is the capability of preventing other parties from learning one's past or current location ..."

- Current HIP architecture does not take into account location privacy
- HIP is an end to end protocol
  - Initiator/Responder learns the location of each other
- Loss of Location Privacy occurs every time a locator parameter is included in HIP procedures
  - Base exchange (R1 and I2 messages)
  - Mobility procedures

Location Privacy Architecture



- Rendezvous Agent (RVA)
  - HI to IP resolution
  - assigns globally routable IP addresses (IPg) to attendants
  - readdresses IPg's to HITs and vice-versa
  - handles local mobility
- RVA Protected Area
  - no IPg are used inside these areas for routing
  - identity based routing (or IPv6)
- RVA Advertisement System
  - Sustained by the AR
  - Announces the AR and RVA Identifiers

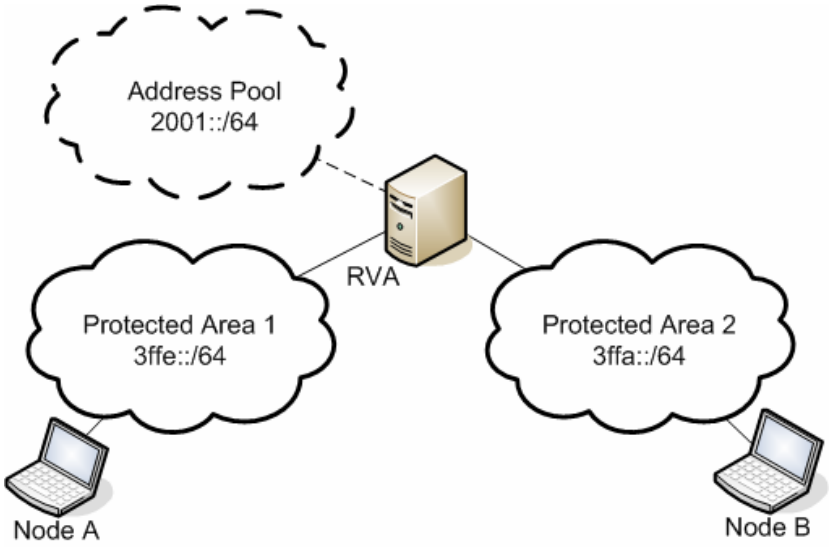
Location Privacy Gains

- Location hidden from end-points
  - Protects from willing and unwilling disclosure
- HMN Location only revealed to eavesdroppers in the AN
  - Layer 2 problem with a Layer 2 solution
- Limited information revealed
  - Global addresses
  - Size of RVA areas determines the amount of geographical information revealed
  - Impossible to see local mobility
  - Possible to see inter RVA movement
    - But just for core network eavesdroppers

IPv6 Instantiation

- IPv6 Access network
- Node acquires Local Address
- Responder sees Global Address
- Address Translation at the RVA
- Neighbor Discovery Protocol (ND) as advertisement system

Prototype Evaluation Scenario



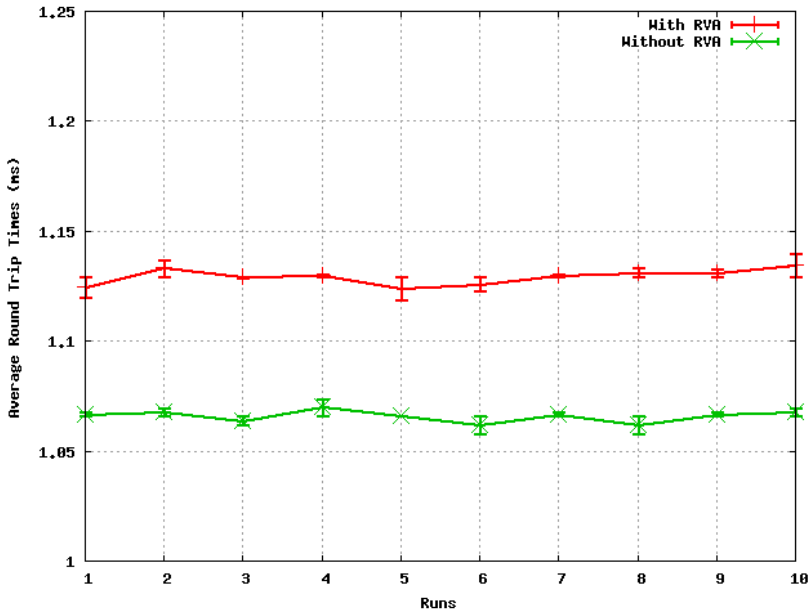
- RVA performs translations for two protected areas
- Node a communicates with node B
- Evaluate Round Trip Time and Bandwidth
- Evaluate leakage of endpoint addresses

Results (I)

Networks	Node A	Node B
Area 1	3ffe::1	2001::6ada:1e65:93f3:ff00
Core	2001::ded8:ce89:6390:eb00	2001::6ada:1e65:93f3:ff00
Area 2	2001::ded8:ce89:6390:eb00	3ffa::1

- Location leakage analysis
  - Node A only sees B's global address
  - Node B only sees A's global address
  - Core network packets only have global addresses
  - Real attachment addresses only "visible" in local network

Results (II)



Average TCP Bandwidth (Mbps/s)	
Without RVA	With RVA
6.43	6.44

- Readdressing performed on all packets
  - Source and destination replacement
- RTT average is only slightly increased
  - Difference of 0.06 ms (on the averages)
- TCP impact is negligible
  - Difference of 0.01 Mbps (on the averages)
- Translations have minimal impacts

Conclusions

- Framework conceals endpoints location
  - Local information contained in protected areas
  - Transport independent (within protected areas)
  - Architecturally supported
- Retains HIP Mobility support
  - But Local Mobility is hidden from peers
- Minimal performance impact
  - Negligible TCP impact
  - Minimum RTT increase (performance can be improved with the assistance of dedicated hardware)
- Requires both sides to implement the framework

Thank you

Questions ?