



# **HIP Privacy Extensions and the Daidalos Approach to HIP**

**19/11/2007, Heidelberg, Germany  
D-AN Workshop**

**Alfredo Matos (IT Aveiro)**

**<alfredo.matos@av.it.pt>**





# Overview

- ▶ HIP in a Daidalos context
- ▶ Privacy in Daidalos
- ▶ HIP Privacy Extensions
- ▶ Daidalos Revised Mobility Architecture
- ▶ Mapping HIP in the new architecture
- ▶ Putting it all together





# Why HIP in a Daidalos context ?

- ▶ Controlled operator environments
  - Previously all MIPv6
  - But we need to push forward (research objectives)
  - Finding better tools for the job
- ▶ Security
- ▶ Mobility
- ▶ Multihoming
  
- ▶ It's all about locator agility and security
  - Locator/Identifier Split





# Daidalos and Privacy

- ▶ User Privacy
  - Fragmented identity model
    - Virtual Identity Framework
  - Many identity and privacy checkpoints
    - Identifier Correlation (today)
    - Vertical Issues
  
- ▶ Location Privacy
  - Achieved with MIPv6 with simple approaches
  - Disabled Route Optimization
  - Reverse tunneling through the Home Agent





# A first look at HIP and Privacy

- ▶ HIP & User Privacy
  - Can be driven by other mechanisms
    - Virtual Identities
  - Strong cryptographic mechanisms
    - Enhance user privacy (by design)
- ▶ HIP & Location privacy
  - Flawed from design
  - HIP is end-to-end
  - Mobility updates directly to peers





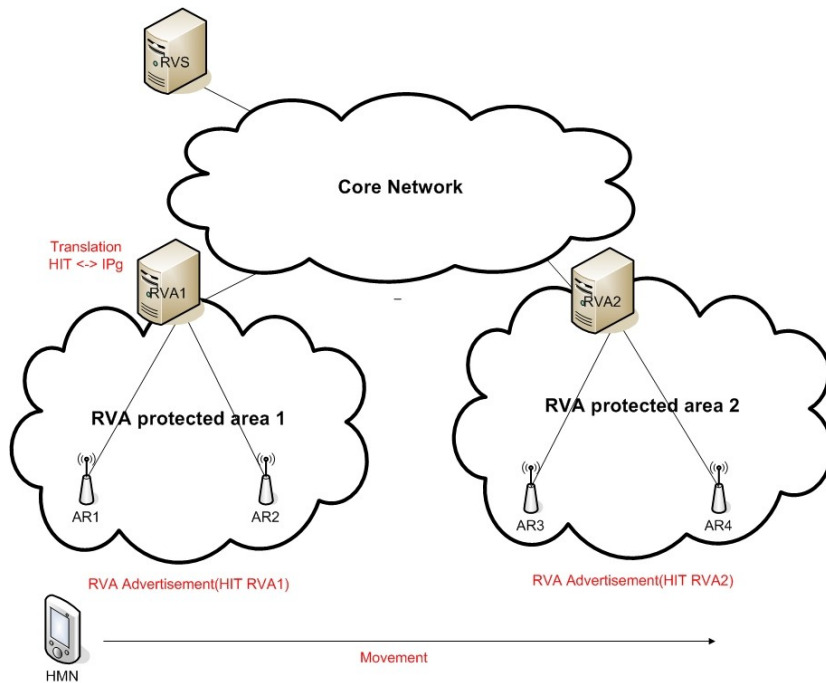
# Daidalos & HIP: privacy requirements

- ▶ First step towards an alternative solution
  - Replace MIPv6 with HIP
  - Retain the MIPv6 benefits
  - Gain on HIP (design) features
  
- ▶ HIP Location Privacy Extensions
  - Enable HIP to provide location privacy to end-points
  - Everything else HIP already supports (with added value)





# HIP Location Privacy Extensions



- ▶ Rendezvous Agent (RVA)
  - HI to IP resolution
  - assigns globally routable IP addresses (IPg) to attendants
  - readdresses IPg's to HITs and vice-versa (or local IPv6 addresses)
  - 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



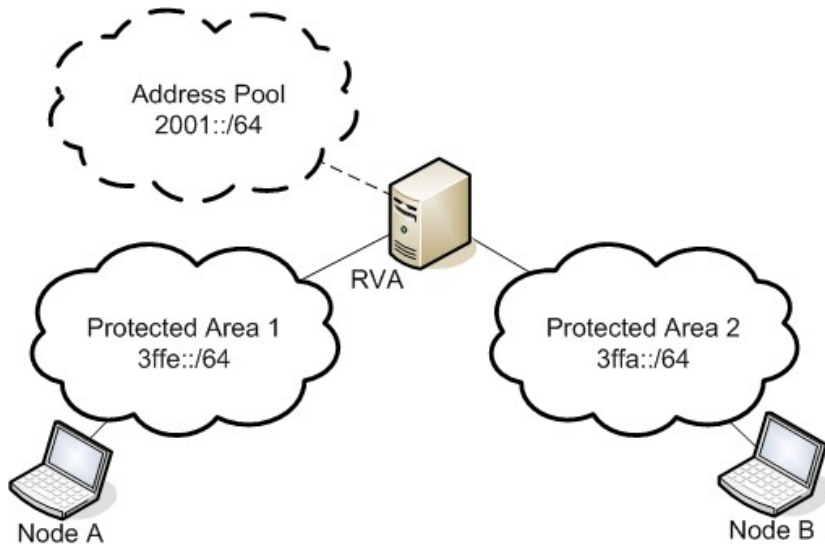
# Location Privacy Gains

- ▶ Location hidden from end-points
- ▶ Location revealed only to attackers on 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;
  - Correspondents do not see local mobility
    - Less updates
    - Faster Mobility
    - Less privacy leakage





# HIP Location Privacy Prototype



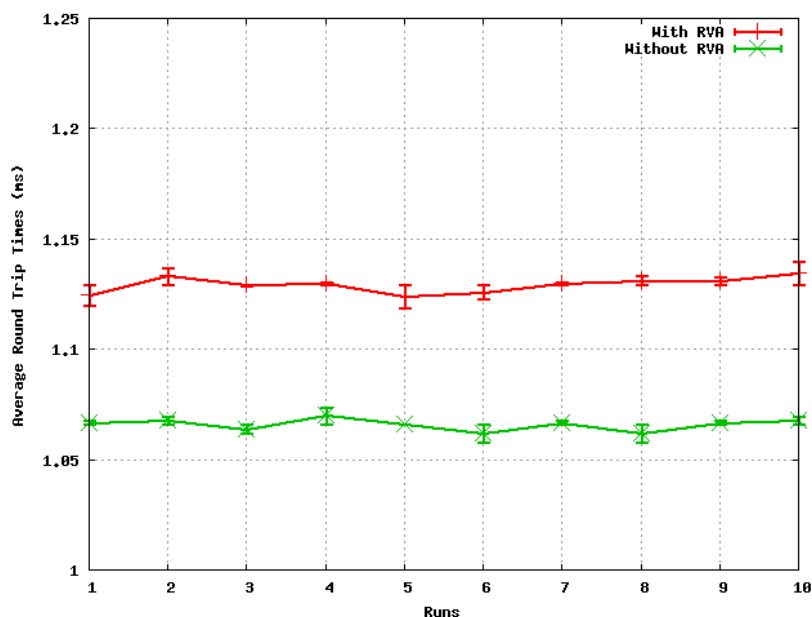
- ▶ Location leakage analysis
- ▶ Node A only sees B's global address
- ▶ Node B only sees A's global address
- ▶ Core network packets only have global addresses
- ▶ Real attachment addresses only "visible" in local network

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





# HIP Location Privacy Prototype Results



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



# Meanwhile... Daidalos Evolved

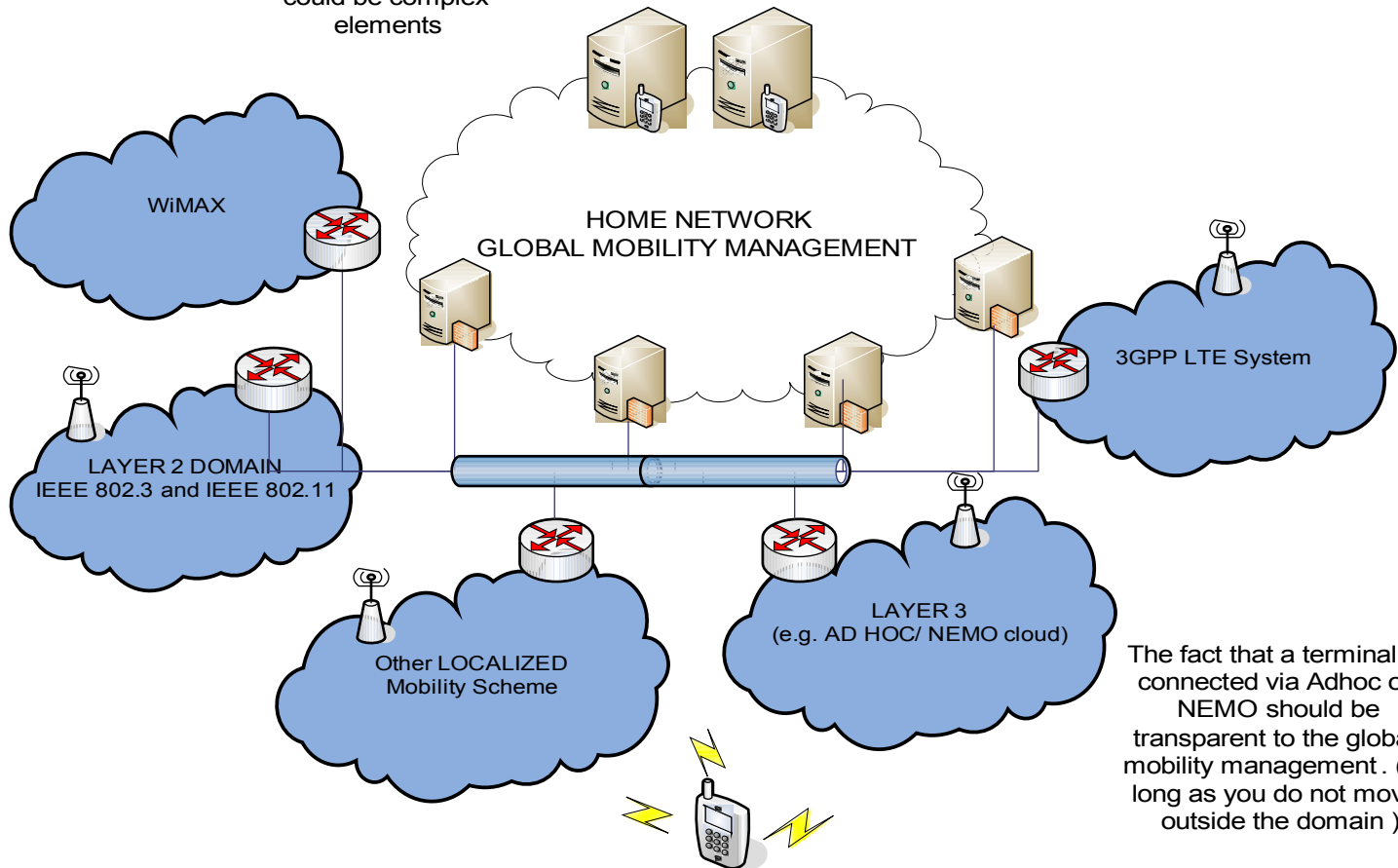
- ▶ Revised Daidalos (II) Architecture
  - Conceptual changes
  - Mobility Paradigm (architectural) shift
- ▶ MobiSplit environment
  - Local Mobility independent of global mobility
  - Local Mobility Domain (LMD)
  - Global Mobility Domain (GMD)
  - Effort to achieve a pluggable architecture





# Mobisplit Overview

The ROUTERS /GW at the edge of the domain could be complex elements



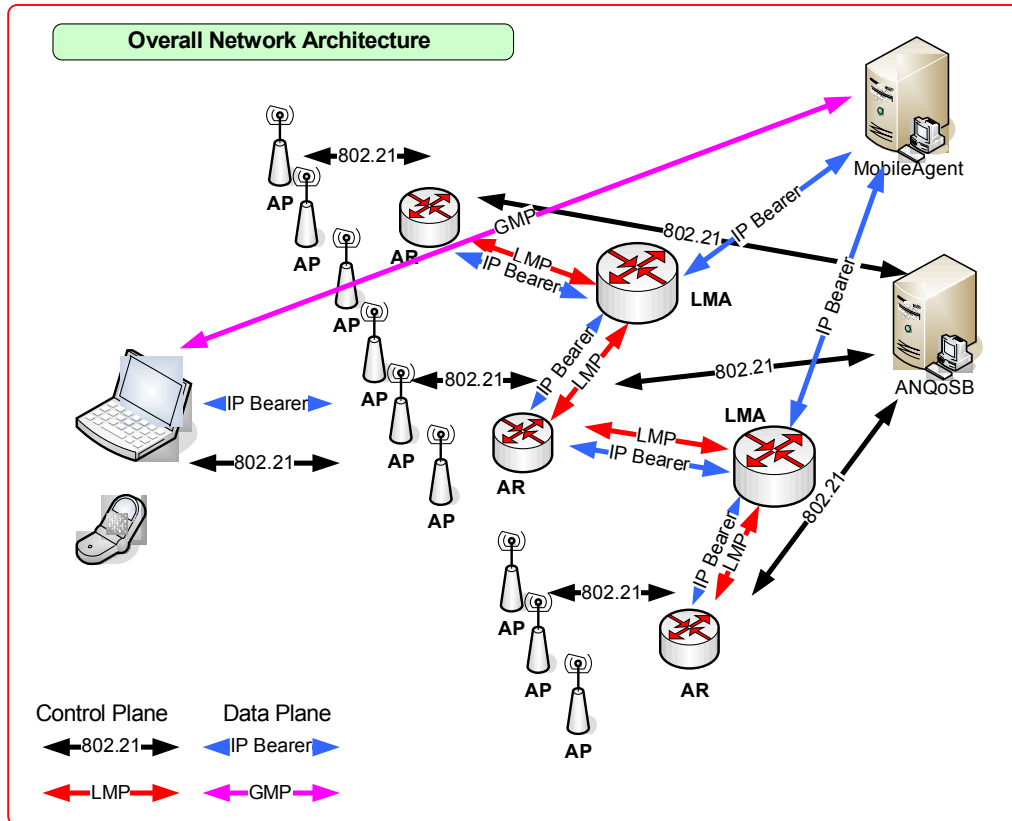
The fact that a terminal is connected via Adhoc or NEMO should be transparent to the global mobility management . (As long as you do not move outside the domain )

MULTIMODE/MULTIHOMED TERMINAL





# Daidalos MobiSplit Architecture



- ▶ **Global Mobility**
  - Main focus on MIPv6
  - Compliance (SDOs)
  - Heritage (D1)
- ▶ **Local Mobility**
  - NetLMM DT draft
  - Revising with PMIPv6
- ▶ **But this is pluggable**
  - Change protocols





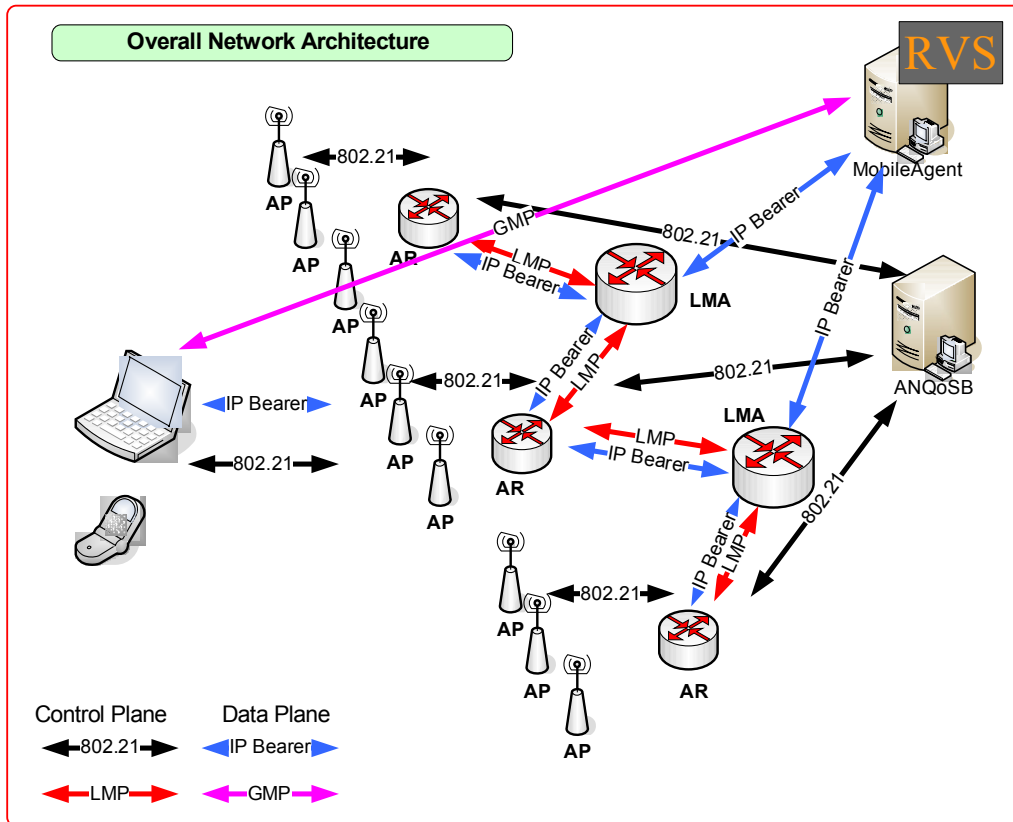
# HIP as a GMD Protocol

- ▶ **MobiSplit provides separation**
  - Local mobility remains independent
  - Global Mobility can be pluggable
- ▶ **Integrating HIP into the architecture**
  - Less constraints (as opposed to privacy extensions)
    - Local domains that provide a degree of Location Privacy
  - Less effort to fit in the architecture
  - Location Privacy protection can be rethought
  - Replace Global Mobility Infrastructure





# Architectural modifications



- ▶ **Architecture**
  - MIPv6 Home Agent dropped
  - Rendezvous Server (RVS) added
- ▶ **Revised architectures**
  - Mobile Terminals
  - Access routers
  - Local Mobility procedures
  - Inter domain mobility
- ▶ **Pluggable is a great idea**
  - But focus is needed



# Identity Framework Integration

- ▶ Coupling HIP with the VID Framework
  - HIP already provides (Host) Identity
  - VID framework provides (User) Identity
  - Two namespaces, one architecture
- ▶ Namespace Merging (or harmonizing)
  - Integrate Host Identity with Virtual Identity
  - Leveraging Private/Public key into the user profile
  - Cross-relationship with other architecture asymmetric crypto systems (e.g. A4C)





# Namespace and ID Model Integration

- ▶ Public Key can be part of Identity Material
  - Stored at an ID Manager/ID Broker
  - Called an Entity Profile Part (ID Model naming)
- ▶ Redesigned HIT to cope with ID Model
  - Integrate with realm
- ▶ Leverage the ID Model by resolving the Realm
  - HIT is the VID Identifier
  - Hash of the HI is the Index at the ID Broker

**HIT = ID Realm | hash(HI)**



# Ongoing Research

- ▶ **Interactions with Location Privacy Framework**
  - Mixing the Daidalos Local Mobility with the HIP oriented approach
  - Overlapping solutions ? Probably not...
    - Pure HIP vs Architecture feature
- ▶ **Mobility**
  - Fix the bits and pieces of Local Mobility Interaction
  - MT-AR Interfaces (with 802.21)
- ▶ **A4C**
  - Integrate HIP Authentication with A4C procedures
  - Leverage existing asymmetric keys
- ▶ **QoS**
  - IPSec and QoS, along with interdomain solutions
  - Flow specific QoS with tunnels





# Conclusions

- ▶ **HIP can provide great value to the Daidalos Architecture**
  - Simplified mobility
  - Added Security
- ▶ **Location Privacy Framework**
  - Conceals end-points
  - Minimal performance impact
  - Retains HIP properties (Mobility, Multihoming, ...)
  - All HIP solution
- ▶ **HIP in the redesigned architecture**
  - Easier to “plugin”
  - Apparent seamless integration, but further study is needed (the dirty work, a.k.a. details)
  - HIP Location Privacy depends on Local Mobility Scheme





**Thank You.**

**Questions ?**

