HIP extensions for object to object communications <draft-lee-hip-object-02.txt>

74th IETF San Francisco, March 2009

Gyu Myoung Lee (gmlee@icu.ac.kr)

Jun Kyun Choi (jkchoi@icu.ac.kr)

Seng Kyoun Jo (skjo@etri.re.kr)

Jeong Yun Kim (jykim@etri.re.kr)

Contents

- ❒ Introduction
- ❒ E-mail discussions since last meeting
- ❒ Updates since -01 version
- ❒ Object mapping – extension of stack architecture
- ❒ Proposals for HIP extensions
- ❒ Protocol operation
- ❒ Issues
- ❒ Next steps

Introduction

- **Object to object communications (ubiquitous networking)**
  - New types of objects connected to the network for enabling the use of various communication services
  - Each object delivers information using network with/without the help of humans. (e.g., sensor networking, etc)
- **Objective**
  - Connecting to anything using object identification
    - Protection of object (including right management)
    - Service and location discovery
- **Solution – HIP extensions**
  - New concept of end points
    - not always humans but may be objects such as devices/machines, and then expanding to small objects and parts of objects
  - Mapping/binding with object identifier

E-mail discussions since last meeting

❒ Detailed protocols

- Mapping between host identity and object identities
  - One-to-one mapping vs. one-to-many mapping
- IPsec security associations
  - Propose alternative solution from Tom
- Detailed protocol operation
  - HIP initiator, HIP responder

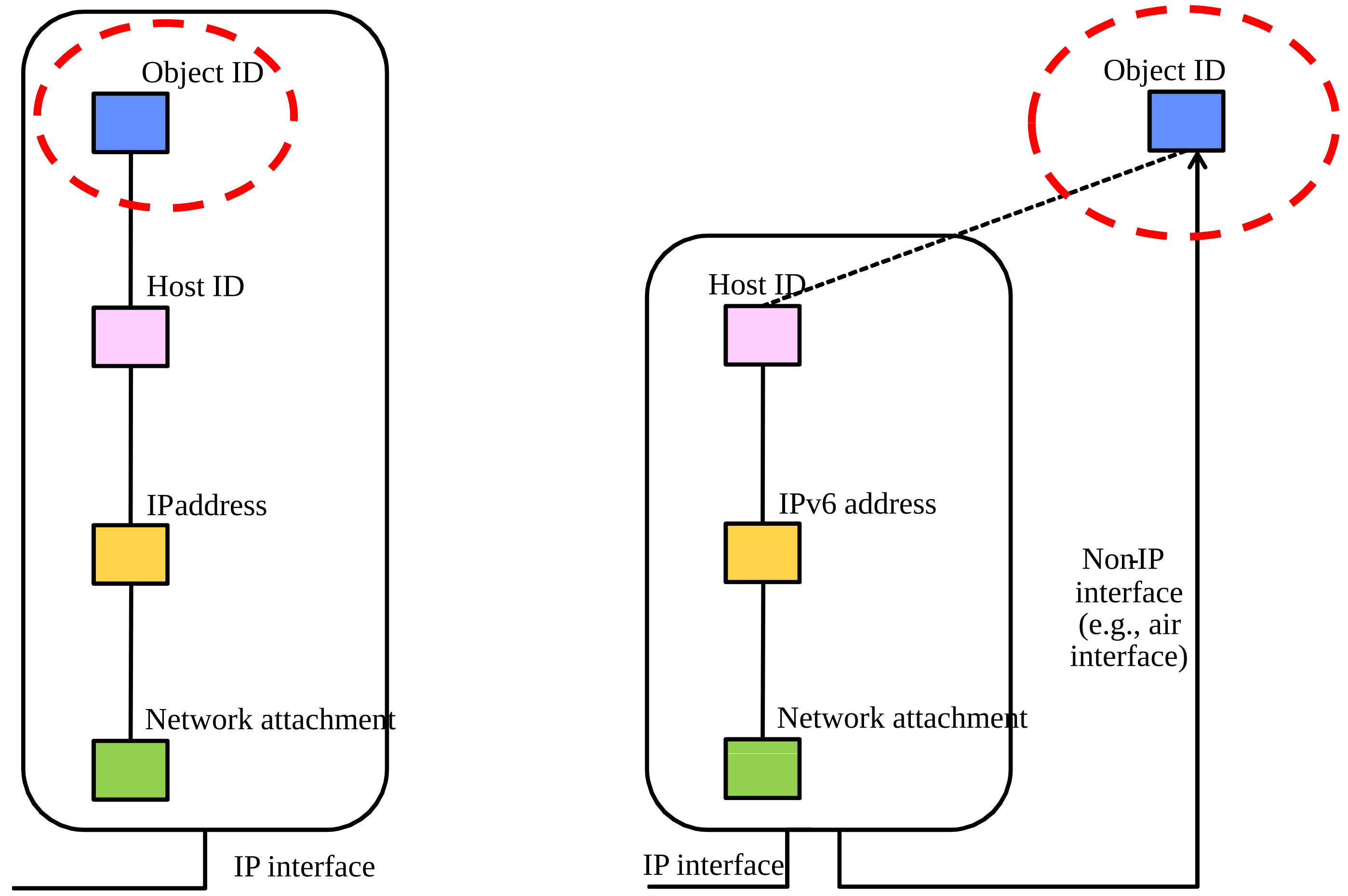
❒ Use case

- The use case of HIP running over a network that is not IP-based
  - RFID reader/tags

Updates since -01 version

- ❒ **Changed parts in -02 version**
  - ● Add **Section 4.3.** object mapping schemes
  - ● Change **Figure 3.** Extension of stack architecture
  - ● Add new proposal for protocol extensions in **Section 5.3.**
  - ● Add **Section 5.4.** Protocol operations and procedures and **Figure 4.**
  - ● Add additional considerations in **Section 6.**

Object mapping – extension of stack architecture



(a) Direct mapping (Object in a host)

(b) Indirect mapping (remote objects)

Proposal #1 for HIP extensions – 1

- Object identity replaces host identity on top of network layer
  - HIP header (include OIT(object identity tag))

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Header   | Header Length |0| Packet Type |  VER. | RES.|1|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Checksum             |           Controls            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Sender's Host/Object Identity Tag (HIT/OIT)           |
|                                                               |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Receiver's Host/Object Identity Tag (HIT/OIT)          |
|                                                               |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
/                        HIP Parameters                         /
/                                                               /
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Proposal #1 for HIP extensions – 2

- New TLV: object_ID
  - Newly defined from HOST_ID of existing HIP
  - The Object Identity is generated from Service IDs defined for specific applications/services

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Type              |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          OI Length            |DI-type|      DI Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Object Identity                         /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                               |        Domain Identifier      /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                               |   Padding     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- How to provide HIP security properties?

Proposal #2 for HIP extensions

❒ Put new name space on top of HIP

- To keep the existing HOST_ID and add new Domain Identifier type for the object ID

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Type              |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          HI Length            |DI-type|     DI Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Host Identity                         /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                               |         Domain Identifier     /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                               |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

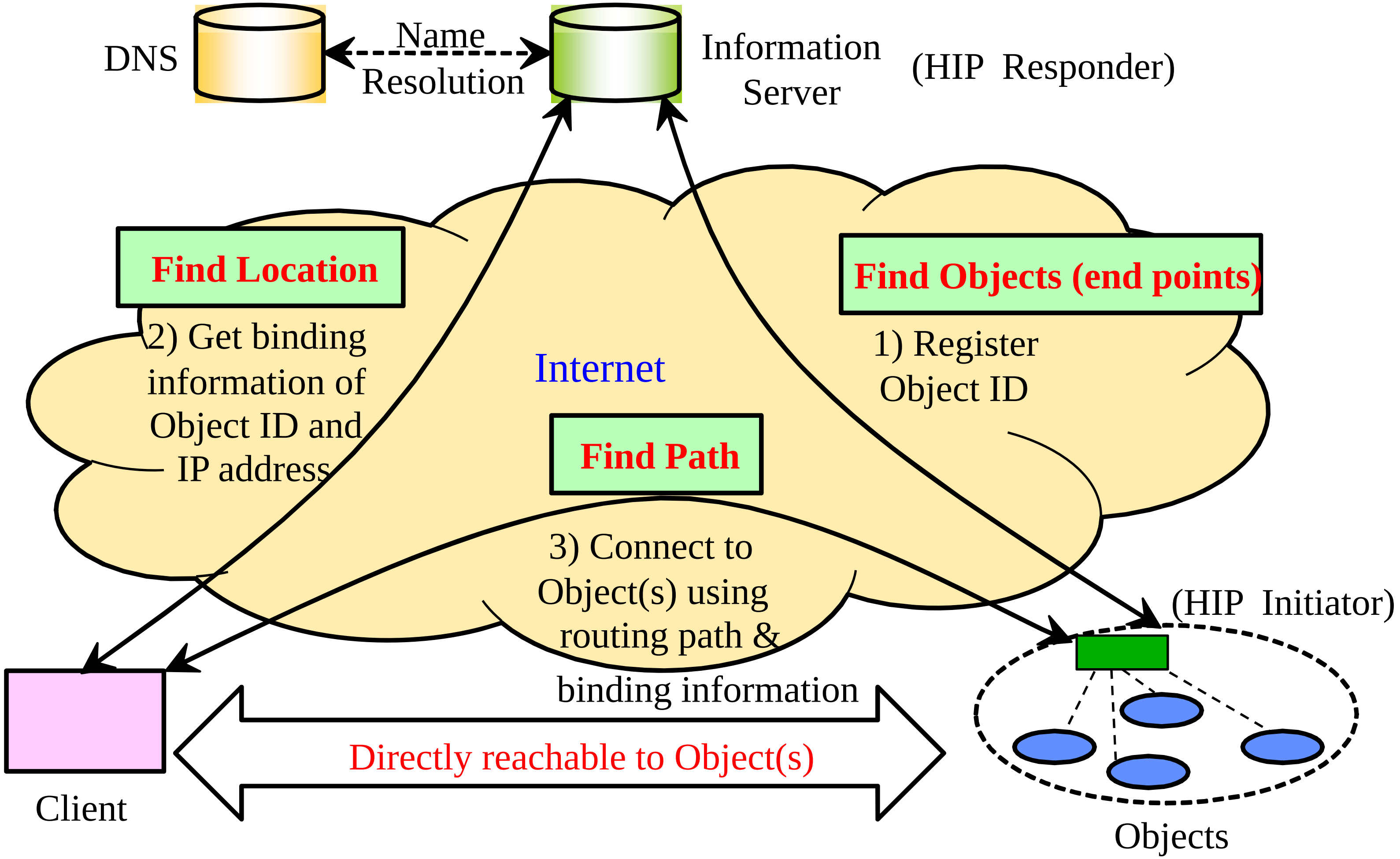
- In this case, we can use the existing HIP for security association
  - Still open issue on security association with object identities

Protocol operation – 1

❒ HIP basic operation (an example of RFID reader/tags)

- HIP Initiator can be a RFID reader which is connected to RFID tags (i.e., objects) using air interface.
- HIP Responder can be the information server which stores all information of RFID tags.
- And then, if this information server has a role of HIP rendezvous server, a client can get binding information between Host (HIP Initiator) and an object behind RFID reader for reachability to object(S) as end point(s).
- The RFID reader has one-to-many mapping relationship. So, a host identity of RFID reader maps onto many object identities.

Protocol operation – 2



DNS

Name Resolution

Information Server

(HIP Responder)

Find Location

2) Get binding information of Object ID and IP address

Internet

Find Path

3) Connect to Object(s) using routing path & binding information

Find Objects (end points)

1) Register Object ID

(HIP Initiator)

Client

Directly reachable to Object(s)

Objects

Issues

- **Security association between object identity and host identity**
  - A host with multiple object identities
    - One host identity, however
    - The granularity and separation of the data flows to be at the object ID level
  - Required abilities
    - The ability that IKEv2 has to establish and maintain multiple security associations (SAs) between hosts
    - The ability to latch these SAs to some higher-level identifiers (e.g., object IDs)
      - Connection latches (IPsec channels): a way to bind the traffic flows for, e.g., TCP connections to security properties desired by the application
- **More detailed use cases**
  - Example: “user Ux with telephone number Nx on host Hx wants to call user Uy at number Ny on host Hy”
    - Application API, protocol stacks, SAs at the granularity of two object IDs

Next steps

❐ Proposal

- Adopt as Research Group Item?
  - Authors would like to propose this to become a research group item
- More contributors for review and great suggestions
  - Please join editing work of this document

❐ Update the document

- From feedbacks and comments in this meeting
  - Protocol solution
  - Use case
- More detailed e-mail discussion with hiprg members