HIP Working Group
Internet-Draft
Expires: December 12, 2005

J. Laganier
DoCoMo Euro-Labs
L. Eggert
NEC

June 10, 2005

Host Identity Protocol (HIP) Rendezvous Extension
draft-ietf-hip-rvs-02

Status of this Memo

Copyright Notice

Abstract

This document discusses a rendezvous extension for the Host Identity Protocol (HIP). The rendezvous extension extends HIP and the HIP registration extension for initiating communication between HIP nodes via HIP rendezvous servers. Rendezvous servers improve reachability and operation when HIP nodes are multi-homed or mobile.

Table of Contents

1. Introduction 3
2. Terminology 4
3. Overview of Rendezvous Server Operation 4
3.1 Diagram Notation 6
3.2 Rendezvous Client Registration 6
3.3 Relaying the Base Exchange 7
4. Rendezvous Server Extensions 8
4.1 LOCATOR Parameter 8
4.2 RENDEZVOUS Registration Type 8
4.3 New Parameter Formats and Processing 9
4.3.1 RVS_HMAC Parameter 9
4.3.2 FROM Parameter 9
4.3.3 VIA_RVS Parameter 10
4.4 Processing Outgoing I1 Packets 10
4.5 Processing Incoming I1 packets 11
5. Security Considerations 11
6. IANA Considerations 12
7. Acknowledgments 12
8. References 13
8.1 Normative References 13
8.2 Informative References 13
Editorial Comments 14
Authors' Addresses 14
A. Document Revision History 14
Intellectual Property and Copyright Statements 16

1. Introduction

The current Internet uses IP addresses for two purposes. First, they are topological locators for network attachment points. Second, they act as names for the attached network interfaces. Saltzer [9] discusses these naming concepts in detail. Routing and other network-layer mechanisms are based on the locator aspects of IP addresses. Transport-layer protocols and mechanisms typically use IP addresses in their role as names for communication endpoints. This dual use of IP addresses limits the flexibility of the Internet architecture. The need to avoid readdressing in order to maintain existing transport-layer connections complicates advanced functionality, such as mobility, multi-homing, or network composition.

The Host Identity Protocol (HIP) architecture [1] defines a new third namespace. The Host Identity namespace decouples the name and locator roles currently filled by IP addresses. Transport-layer mechanisms operate on Host Identities instead of using IP addresses as endpoint names. Network-layer mechanisms continue to use IP addresses as pure locators. Because of this decoupling the HIP layer needs to map Host Identities into IP addresses.

Without HIP, a node needs to know its peer's IP address to make initial contact. The Host Identity Protocol architecture [1] does not change this basic property, but introduces an additional, optional piece of infrastructure, the rendezvous server (RVS). An RVS serves as an additional initial contact point ("rendezvous point") for its clients. The clients of an RVS are HIP nodes that use the HIP Registration Protocol [2] to register their HIT->IP address mappings with the RVS. After this registration, other HIP nodes can initiate a base exchange using the IP address of the RVS instead of the current IP address of the node they attempt to contact. Essentially, the clients of an RVS become reachable at the RVS' IP addresses. Peers can initiate a HIP base exchange with the IP address of the RVS, which will relay this initial communication such that the base exchange may successfully complete.

When HIP nodes frequently change their network attachment points, using a RVS can improve reachability and operation. Without an RVS, a HIP node needs to update its DNS entry with its current IP address before it becomes reachable to its peers. Although the DNS offers mechanisms for dynamic updates to records[10][11], they may not be suitable when a record changes frequently. Caching, state lifetimes and deficiences in existing DNS implementations limit the rate-of-change for a given record. When using an RVS - which is assumed to be reachable at a static or at least infrequently changing IP address - HIP nodes need not update their DNS records whenever their local IP

addresses change. Instead, they register the IP address of their RVS in their DNS entry and then update only their RVS when their IP addresses change. Because the RVS is specifically designed to support high-rate updates, this indirection can improve reachability of HIP nodes.

2. Terminology

This section defines terms used throughout the remainder of this specification.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [3].

In addition to the terminology defined in [2], this document defines and uses the following terms:

Rendezvous Service
: A HIP service provided by a rendezvous server to its rendezvous clients. The rendezvous server offers to relay some of the arriving base exchange packets between the initiator and responder. [Comment.1]

Rendezvous Server (RVS)
: A HIP registrar providing rendezvous service.

Rendezvous Client
: A HIP requester that has registered for rendezvous service at a

rendezvous server.

Rendezvous Registration
A HIP registration for rendezvous service, established between a rendezvous server and a rendezvous client.

3. Overview of Rendezvous Server Operation

HIP decouples domain names from IP addresses. Because transport protocols bind to host identities, they remain unaware if the set of IP addresses associated with a host identity changes. This change can have various reasons, including, but not limited to, mobility and multi-homing.


```
+------+                 +------+
|      |-------I1------>|      |
|  I   |<-------R1-------|  R   |
|      |-------I2------>|      |
|      |<-------R2-------|      |
+------+                 +------+
```

Figure 1: HIP base exchange without rendezvous server.

Figure 2 shows a simple HIP base exchange without a rendezvous server, in which the initiator initiates the exchange directly with the responder by sending an I1 packet to the responder's IP address, as per the HIP base specification [4].

Proposed extensions for mobility and multi-homing [5] allow a HIP node to notify its peers about changes in its set of IP addresses. These extensions require an established HIP association between two nodes, i.e., a completed HIP base exchange.

However, such a HIP node MAY also want to be reachable to other future correspondent peers that are unaware of its location change. The HIP architecture [1] introduces rendezvous servers with whom a

HIP node MAY register its host identity tags (HITs) and current IP addresses. An RVS relays HIP packets arriving for these HITs to the node's registered IP addresses. When a HIP node has registered with an RVS, it SHOULD record the IP address of its RVS in its DNS record, using the HIPRVS DNS record type defined in [12].

```
                  +-----+
         +--I1--->| RVS |---I1--+
         |        +-----+       |
         |                      v
      +-----+                +-----+
      |     |<------R1-------|     |
      |  I  |-------I2------>|  R  |
      |     |<------R2-------|     |
      +-----+                +-----+
```

Figure 2: HIP base exchange with a rendezvous server.

Figure 2 shows a HIP base exchange involving a rendezvous server. It is assumed that HIP node R previously registered its HITs and current IP addresses with the RVS, using the HIP registration protocol [2]. When the initiator I tries to establish contact with the responder R, it MAY send the I1 of the base exchange either to one of R's DNS addresses or it MAY send it to the address of one of R's rendezvous servers instead. Here, I obtains the IP address of R's rendezvous server from R's DNS record and then sends the I1 packet of the HIP

base exchange to RVS. RVS, noticing that the HIT contained in the arriving I1 packet is not one of its own, MUST check its current registrations to determine if if needs to relay the packets. Here, it determines that the HIT belongs to R and then relays the I1 packet to the registered IP address. R then completes the base exchange without further assistance from RVS by sending an R1 directly to the I's IP address, as obtained from the I1 packet.

3.1 Diagram Notation

Notation	Significance
I, R	I and R are the respective source and destination IP addresses in the IP header.

HIT-I, HIT-R   HIT-I and HIT-R are the initiator's and the responder's HITs in the packet, respectively.

LOC:I   A LOCATOR parameter containing the IP address I is present in the HIP header.

FROM:I   A FROM parameter containing the IP address I is present in the HIP header.

VIA:RVS   A VIA_RVS parameter containing the IP addresses of an RVS is present in the HIP header.

REG_REQ   A REG_REQUEST parameter is present in the HIP header.

REG_RES   A REG_RESPONSE parameter is present in the HIP header.

3.2 Rendezvous Client Registration

Before a rendezvous server starts to relay HIP packets to a rendezvous client, the rendezvous client needs to register with it to receive rendezvous service by using the HIP registration extension [2] as illustrated in the following schema:


```
+-----+                             +-----+
|     |              I1             |     |
|     |---------------------------->|     |
|     |<----------------------------|     |
|  I  |         R1(REG_INFO)        | RVS |
|     |         I2(REG_REQ)         |     |
|     |---------------------------->|     |
|     |<----------------------------|     |
```

```
                |      |          R2(REG_RES)          |      |
                +------+                               +------+
```

3.3 Relaying the Base Exchange

If a HIP node and one of its rendezvous servers have a rendezvous registration, the rendezvous servers MUST relay inbound I1 packets that contain one of the client's HITs by rewriting the IP header. They replace the destination IP address of the I1 packet with one of the IP addresses of the owner of the HIT, i.e., the rendezvous client. They MUST also recompute the IP checksum accordingly.

Because of egress filtering on the path from the RVS to the client, a HIP rendezvous server MAY also need to replace the source IP address, i.e., the IP address of I, with one of its own IP addresses. The replacement IP address SHOULD be chosen according to [6] and, when IPv6 is used, to [7]. Because this replacement conceals the initiator's IP address, the RVS MUST append a FROM parameter containing the original source IP address of the packet. This FROM parameter MUST be integrity protected by a RVS_HMAC keyed with the corresponding rendezvous registration integrity key [2].

```
                                             I1(RVS, R, HIT-I, HIT-R
         I1(I, RVS, HIT-I, HIT-R) +---------+     FROM:I, VIA:RVS)
         +----------------------->|         |--------------------+
         |                        |   RVS   |                    |
         |                        |         |                    |
         |                        +---------+                    |
         |                                                       V
        +-----+        R1(R, I, HIT-R, HIT-I, LOC:R, VIA:RVS)  +-----+
        |     |<---------------------------------------------|     |
        |     |                                              |     |
        |  I  |            I2(I, R, HIT-I, HIT-R)            |  R  |
        |     |--------------------------------------------->|     |
        |     |<---------------------------------------------|     |
        +-----+             R2(R, I, HIT-R, HIT-I)           +-----+
```

Figure 5: Rendezvous server rewriting IP addresses

This modification of HIP packets at a rendezvous server can be problematic. The HIP protocol uses two kinds of packet integrity checks: hop-by-hop and end-to-end. The HIP checksum is a hop-by-hop check and SHOULD be verified and recomputed by each of the on-path HIP-enabled middleboxes, such as rendezvous servers. The HMAC and SIGNATURE are end-to-end checks and MUST be computed by the sender and verified by the receiver.

The RVS MUST verify the checksum field of an I1 packet doing any modifications. After modification, it MUST recompute the checksum field using the updated HIP header, which possibly included new FROM and RVS_HMAC parameters, and a pseudo-header containing the updated source and destination IP addresses. This enables the responder to validate the checksum of the I1 packet "as is", without having to parse any FROM parameters.

The SIGNATURE and HMAC verification MUST NOT cover any FROM and RVS_HMAC parameters added by rendezvous servers. Hence, HMAC and SIGNATURE are unaffected by the modifications performed by an RVS. The computation and verification of HMAC and SIGNATURE MUST only cover the original HIP header with a checksum field set to zero, MUST NOT cover the pseudo header that contains modified IP addresses, and mUST NOT cover any new FROM and RVS_HMAC parameters that MAY be situated after the HMAC and SIGNATURE in the HIP header.

4. Rendezvous Server Extensions

The following sections describe extensions to the HIP registration protocol [2], allowing a HIP node to register with a rendezvous server for rendezvous service and notify the RVS aware of changes to its current location. It also describes an extension to the HIP protocol [4] itself, allowing establishment of HIP associations via one or more HIP rendezvous server(s).

4.1 LOCATOR Parameter

A HIP responder contacted via an RVS MAY use a LOCATOR parameter in the R1 packet to notify the initiator of its current IP address, in conformance with the guidelines specified in [5].

4.2 RENDEZVOUS Registration Type

This specification defines an additional registration for the HIP registration protocol [2] that allows registering with a rendezvous server for rendezvous service.

```
Number   Registration Type
------   -----------------
```

```
   1        RENDEZVOUS
```

4.3 New Parameter Formats and Processing

4.3.1 RVS_HMAC Parameter

The RVS_HMAC is an OPTIONAL parameter whose only difference with the HMAC parameter defined in [4] is its "type" code. This change causes it to be located after the FROM parameter (as opposed to the HMAC):

```
   Type         [ TBD by IANA (65472 = 2^16 - 2^6) ]
   Length       20
   HMAC         160 low order bits of a HMAC keyed with the
                appropriate HIP integrity key (HIP_lg or HIP_gl),
                established when rendezvous registration happened.
                This HMAC is computed over the HIP packet, excluding
                RVS_HMAC and any following parameters. The
                "checksum" field MUST be set to zero and the HIP header
                length in the HIP common header MUST be calculated
                not to cover any excluded parameter when the
                "authenticator" field is calculated.
```

To allow a rendezvous client and its RVS to verify the integrity of packets flowing between them, both SHOULD protect packets with an added RVS_HMAC parameter keyed with the HIP_lg or HIP_gl integrity key. A valid RVS_HMAC SHOULD be present on every packets flowing between a client and a server and MUST be present when a FROM parameters is processed.

4.3.2 FROM Parameter

```
    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            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                             Address                           |
   |                                                               |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

   Type         [ TBD by IANA (65470 = 2^16 - 2^6 - 2) ]
   Length       16
   Address      An IPv6 address or an IPv4-in-IPv6 format IPv4 address.
```

A rendezvous server MUST add a FROM parameter containing the original

source IP address of a HIP packet whenever the source IP address in the IP header is rewritten. If one or more FROM parameters are already present, the new FROM parameter MUST be appended after the existing ones.

Whenever an RVS inserts a FROM parameter, it MUST insert an RVS_HMAC protecting the packet integrity, especially the IP address included in the FROM parameter.

4.3.3 VIA_RVS Parameter

```
     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            |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    |                            Address                            |
    |                                                               |
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    .                               .                               .
    .                               .                               .
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    |                            Address                            |
    |                                                               |
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

    Type         [ TBD by IANA (65474 = 2^16 - 2^6 + 2) ]
    Length       Variable
    Address      An IPv6 address or an IPv4-in-IPv6 format IPv4 address
```

After the responder receives a relayed I1 packet, it can begin to send HIP packets addressed to the initiator's IP address, without further assistance from an RVS. For debugging purposes, it MAY include a subset of the IP addresses of its RVSs in some of these packets. When a responder does so, it MUST append a newly created

VIA_RVS parameter at the end of the HIP packet. The main goal of using the VIA_RVS parameter is to allow operators to diagnose possible issues encountered while establishing a HIP association via a RVS.

4.4 Processing Outgoing I1 Packets

An initiator SHOULD not send an opportunistic I1 with a NULL destination HIT to an IP address which is known to be a rendezvous

server address, unless it wants to establish a HIP association with the rendezvous server itself and does not know its HIT.

If an RVS needs to rewrite the source IP address of an I1 packet due to egress filtering, then it MUST add a FROM parameter to the I1 that contasins the initiator's source IP address. This FROM parameter MUST be protected by a RVS_HMAC keyed with the integrity key established at rendezvous registration.

4.5 Processing Incoming I1 packets

When a rendezvous server receives an I1 whose destination HIT is not its own, it MUST consult its registration database to find a registration for the rendezvous service established by the HIT owner. If it finds an appropriate registration, it MUST relay the packet to the registered IP address. If it does not find an appropriate registration, is MUST drop the packet.

A rendezvous server SHOULD interpret any incoming opportunistic I1 (i.e., an I1 with a NULL destination HIT) as an I1 addressed to itself and SHOULD NOT attempt to relay it to one of its clients.

When a rendezvous client receives an I1, it MUST validate any present RVS_HMAC parameter. If the RVS_HMAC cannot be verified, the packet SHOULD be dropped. If the RVS_HMAC cannot be verified and a FROM parameter is present, the packet MUST be dropped.

A rendezvous client acting as responder SHOULD drop opportunistic I1s that include a FROM parameter, because this indicates that the I1 has been relayed.

5. Security Considerations

The security aspects of different HIP rendezvous mechanisms are currently being investigated. This section describes the known threats introduced by these HIP extensions and implications on the overall security of HIP and IP. In particular, it argues that the extensions described in this document do not introduce additional threats to the Internet infrastructure.

It is difficult to encompass the whole scope of threats introduced by rendezvous servers, because their presence has implications both at the IP and HIP layers. In particular, these extensions might allow for redirection, amplification and reflection attacks at the IP layer, as well as attacks on the HIP layer itself, for example, man-in-the-middle attacks against HIP's SIGMA protocol.

If an initiator has a priori knowledge of the responder's host

identity when it first contacts it via an RVS, it has a means to verify the signatures in the HIP exchange, thus conforming to the SIGMA protocol which is resilient to man-in-the-middle attacks.

If an initiator does not have a priori knowledge of the responder's host identiy (so-called "opportunistic initiators"), it is almost impossible to defend the HIP exchange against these attacks, because the public keys exchanged cannot be authenticated. The only approach would be to mitigate hijacking threats on HIP state by requiring an R1 answering an opportunistic I1 to come from the same IP address that originally sent the I1. This procedure retains a level of security which is equivalent to what exists in the Internet today.

However, for reasons of simplicity, this specification does not allow to establish a HIP association via a rendezvous server in an opportunistic manner.

6. IANA Considerations

This section is to be interpreted according to [8].

This document updates the IANA Registry for HIP Parameters Types by assigning new HIP Parameter Types values for the new HIP Parameters defined in Section 4.3:

o RVS_HMAC (defined in Section 4.3.1)

o FROM (defined in Section 4.3.2)

o VIA_RVS (defined in Section 4.3.3)

7. Acknowledgments

The following people have provided thoughtful and helpful discussions and/or suggestions that have improved this document: Marcus Brunner, Tom Henderson, Miika Komu, Mika Kousa, Pekka Nikander, Justino Santos, Simon Schuetz, Tim Shepard, Kristian Slavov, Martin Stiemerling and Juergen Quittek.

Lars Eggert is partly funded by Ambient Networks, a research project supported by the European Commission under its Sixth Framework Program. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Ambient Networks project or the European Commission.

8. References

8.1 Normative References

[1] Moskowitz, R., "Host Identity Protocol Architecture", draft-ietf-hip-arch-02 (work in progress), January 2005.

[2] Koponen, T. and L. Eggert, "Host Identity Protocol (HIP) Registration Extension", draft-koponen-hip-registration-00 (work in progress), February 2005.

[3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[4] Moskowitz, R., "Host Identity Protocol", draft-ietf-hip-base-02 (work in progress), February 2005.

[5] Nikander, P., "End-Host Mobility and Multi-Homing with Host Identity Protocol", draft-ietf-hip-mm-01 (work in progress), February 2005.

[6] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

[7] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[8] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

8.2 Informative References

[9] Saltzer, J., "On the Naming and Binding of Network Destinations", RFC 1498, August 1993.

[10] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[11] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.

[12] Nikander, P. and J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions", draft-ietf-hip-dns-01 (work in progress), February 2005.

[13] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[14] Killalea, T., "Recommended Internet Service Provider Security Services and Procedures", BCP 46, RFC 3013, November 2000.

Editorial Comments

[Comment.1] In this specification the client of the RVS is always the responder. However, there might be reasons to allow a client to initiate a base exchange through its own RVS, like NAT and firewall traversal. This specification does not address such scenarios which should be specified in other documents.

Authors' Addresses

Julien Laganier
DoCoMo Communications Laboratories Europe GmbH
Landsberger Strasse 312
Munich 80687
Germany

Phone: +49 89 56824 231
Email: julien.ietf@laposte.net
URI: http://www.docomolab-euro.com/

Lars Eggert
NEC Network Laboratories
Kurfuerstenanlage 36
Heidelberg 69115
Germany

Phone: +49 6221 90511 43
Fax: +49 6221 90511 55
Email: lars.eggert@netlab.nec.de
URI: http://www.netlab.nec.de/

Appendix A. Document Revision History

Revision	Comments
02	Removed multiple relaying techniques but simple I1 header rewriting. Updated new HIP parameters type numbers (consistent with new layout and assigning rules from draft-ietf-hip-base.) Updated IANA Considerations.

01	Splitted out the registration sub-protocol. Simplify typology of relaying techniques (keep only TUNNEL, REWRITE, BIDIRECTIONAL). Rewrote IANA Considerations.
00	Initial version as a HIP WG item.

```
+----------+---------------------------------------------------+
```

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.